2022 Annual

Blockchain Security and AML Analysis Report

SLOWMIST

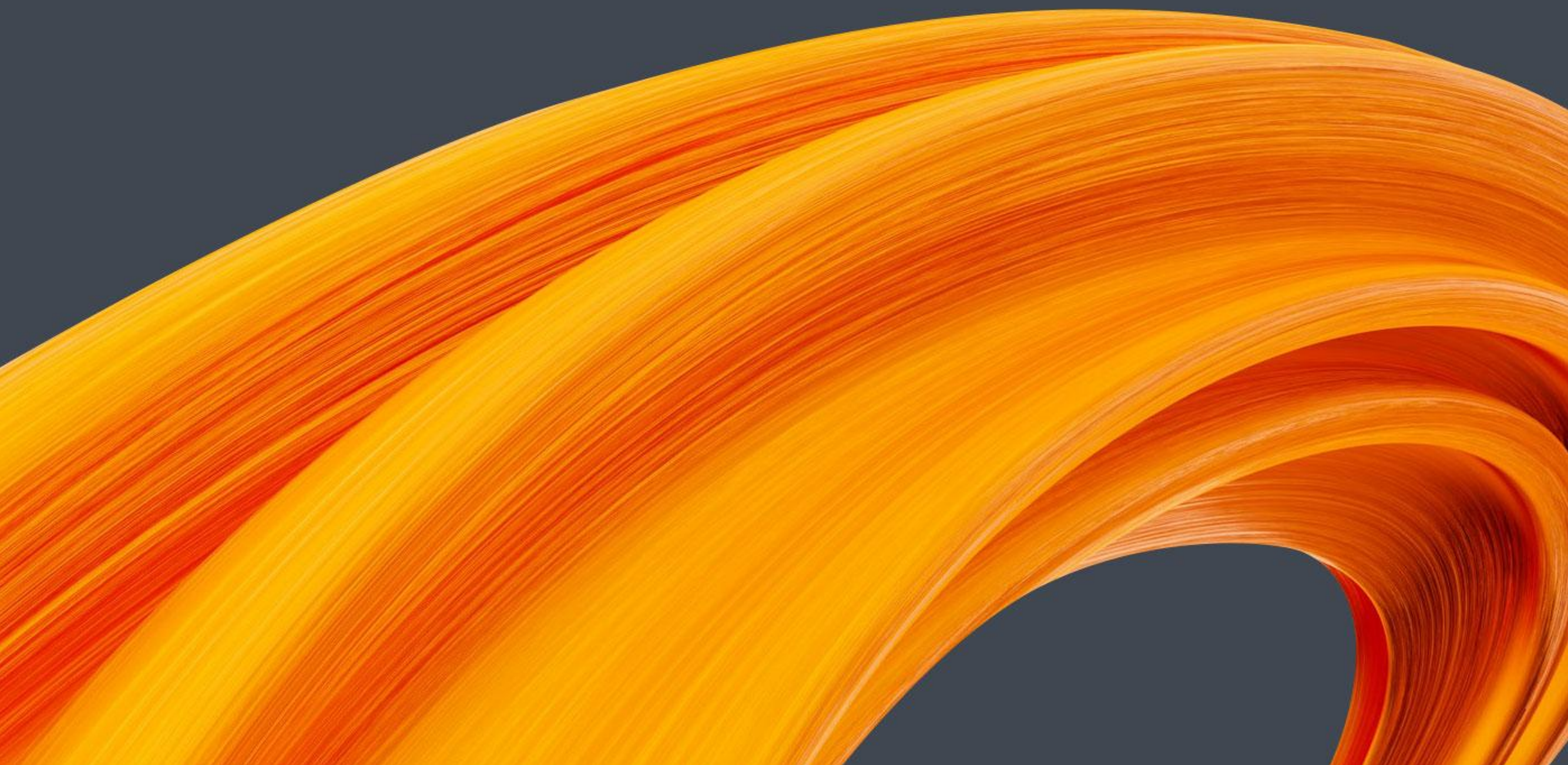


Table of Contents

This report takes a close look at the major events in the blockchain industry that took place in 2022. It provides an overview of the security status of each area within the industry and delves into common attack techniques. Additionally, it uncovers a few phishing techniques and analyzes the flow of stolen funds in some security incidents. To round things off, the report introduces an advanced method for tracking coin mixer funds through a comprehensive analysis.

I. Background

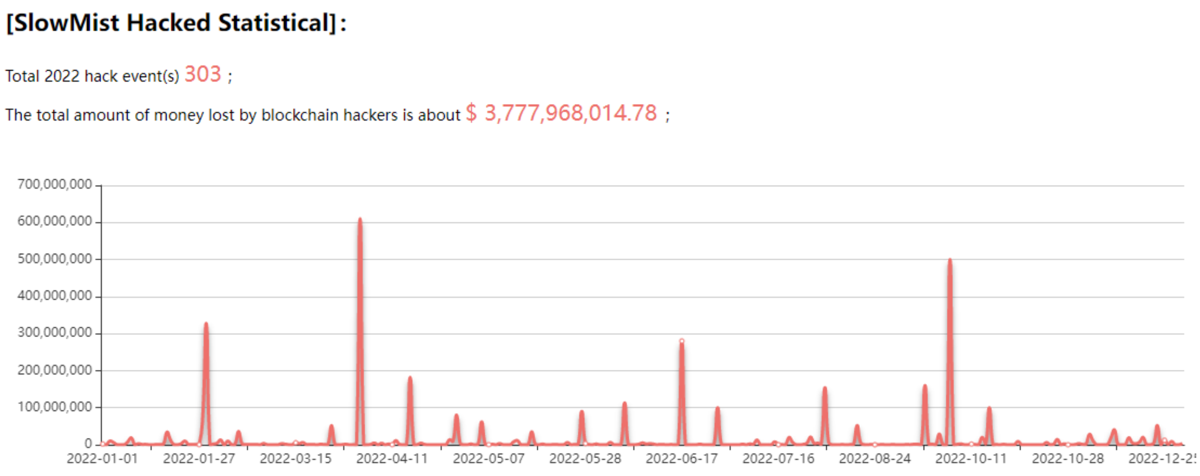
At the beginning of 2022, the global cryptocurrency market had a total capitalization of nearly $3 trillion, leading many to believe that the industry would continue to thrive and attract more hopeful investors. However, several major events shook the market and disrupted the confidence of some participants. These included significant price drops and the collapse of exchanges such as Terra, Celsius Network, Voyager Digital, Three Arrows Capital, and FTX, which caused the total market capitalization of the entire cryptocurrency market to plummet by $2 trillion.

Despite the challenges faced in 2022, there were also some promising developments in the industry. One notable event was the successful merger of Ethereum on September 15, which marked an important step towards solving the scalability problem on the Ethereum blockchain. On July 4, the European Union established the first set of cryptocurrency regulation rules. Additionally, the official launch of the Cosmos White Paper 2.0 at Cosmoverse on September 27 signaled the official entry of Cosmos into the 2.0 era. We also saw the emergence of many new trends and themes, an increase in the number of cryptocurrency users and Web3 developers, and the beginnings of the metaverse. Furthermore, the blockchain industry is at the beginning of a new era of cryptocurrency regulation, with the market moving toward compliance. These trends are expected to continue driving the industry in 2023 and beyond.

Overall, 2022 was a tumultuous yet hopeful year for the blockchain industry. This report will review the significant security events and anti-money laundering efforts that took place within the industry in 2022, while also considering the trends and developments that are expected to shape the industry in the coming year. By examining the successes and setbacks of the past year, we can better understand the dynamic nature of the blockchain industry and look forward to a promising future.

1.1 Blockchain Security

According to SlowMist Hacked, a database of blockchain security incidents, there were 303 blockchain-related security incidents in 2022, resulting in losses of up to $3.777 billion (calculated at the price at the time of the event).



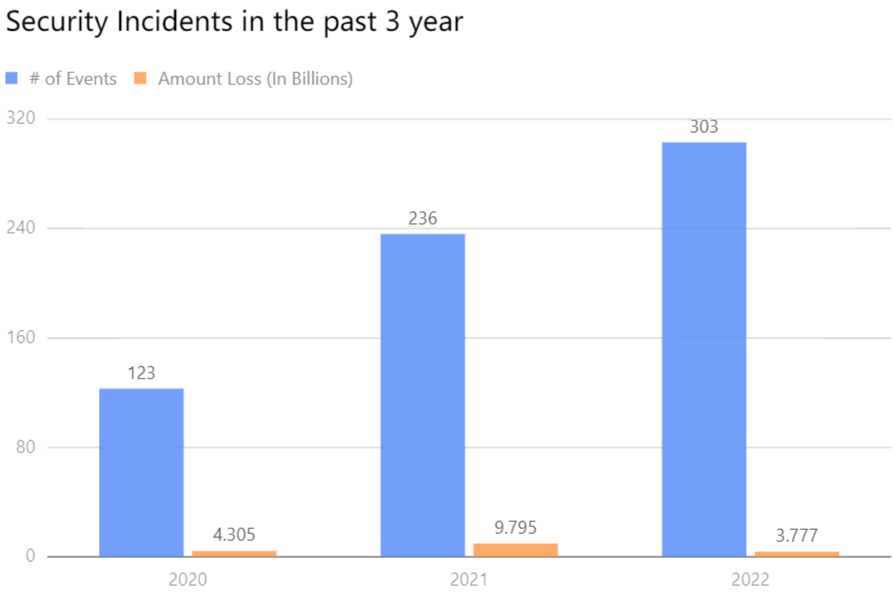
[SlowMist Hacked Statistical]:

Total 2022 hack event(s) 303 ;

The total amount of money lost by blockchain hackers is about $ 3,777,968,014.78 ;

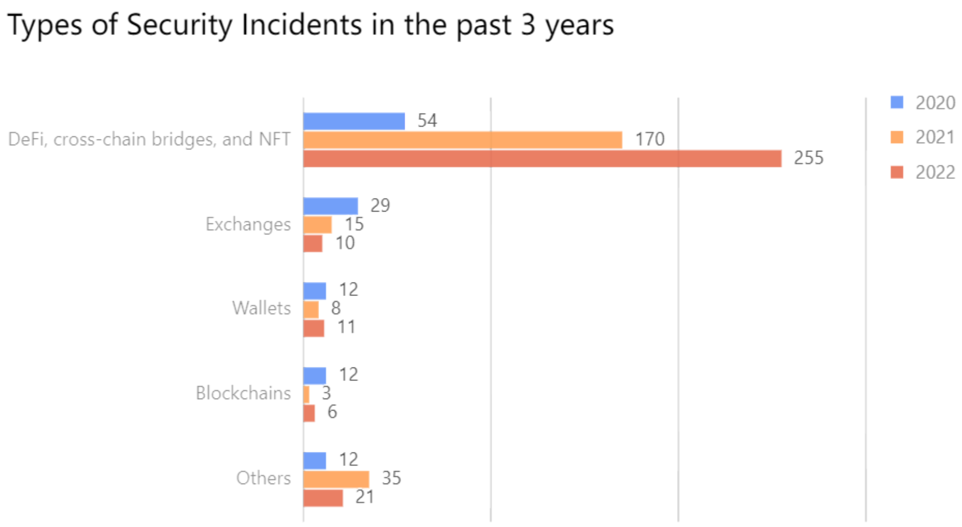
(2022 Security Incident Statistics)

It is worth noting that the $3.777 billion in losses reported by SlowMist Hacked represents a 61% decrease from the $9.795 billion in losses seen in 2021. However, it should be noted that this figure does not take into account assets lost due to market instability, and this figure is also affected by currency prices.



(Comparison of blockchain losses over the past 3 years)

There were a total of 255 security incidents affecting various ecosystems, including DeFi, cross-chain bridges, and NFT. Additionally, there were 10 security incidents involving exchanges, 11 incidents involving public chains, 6 incidents involving wallets, and 21 incidents of other types.



(A comparison of security incidents on different trajectories over the past 3 years)

1.2 Blockchain Anti-Money Laundering

Cryptocurrency transactions are inherently anonymous and irreversible, making it particularly important to implement effective measures for blockchain anti-money laundering in order to prevent hackers from profiting from their crimes. In response to this ongoing threat, various groups, including trading platforms/fund management platforms/projects, regulators, and blockchain security companies, have formed anti-money laundering alliances to combat this issue.

In 2022, the anti-money laundering dynamics for these groups were as follows:

Trading platforms/fund management platforms/projects:
Tether: In 2022, a total of 250 ETH addresses were blocked, and the USDT-ERC20 assets on these addresses were frozen and unable to be transferred.
Circle: In 2022, a total of 126 ETH addresses were blocked, and the USDC-ERC20 funds on these addresses were frozen and unable to be transferred.

Regulators:
Federal Bureau of Investigation: On February 18, it announced the creation of a new Virtual Assets Unit to centralize its response to the sprawling field of crypto-based crime.

US Department of Treasury: On April 14, it imposed sanctions on addresses related to the Ronin Network hackers (LAZARUS GROUP), and on May 6, it imposed sanctions on the cryptocurrency mixer Blender. This marked the first time that the US Department of Treasury had ever imposed sanctions on a cryptocurrency mixer platform. On August 8, it imposed sanctions on the Ethereum cryptocurrency mixer Tornado.Cash, and sanctioned 38 addresses.

US Department of Justice: On Sept 17, it launched a national network of prosecutors focused on fighting cryptocurrency crime.

Blockchain Security Companies:

Chainalysis: On March 10, it created the SanctionsList on-chain database contract, which included the blacklisting of a total of 177 addresses.

SlowMist: On April 27, its MistTrack anti-money laundering tracking system was officially launched, focusing on the crackdown of cryptocurrency money laundering activities.

It is well known that hackers, black market groups, fraudsters, and Rug Pull project players have been the main forces behind money laundering, with the most infamous being the North Korean LAZARUS GROUP hacker organization, which poses a major threat to the security of the blockchain ecosystem.

Based on open-source intelligence and on-chain data analytics, the dynamics of LAZARUS GROUP in 2022 are as follows:

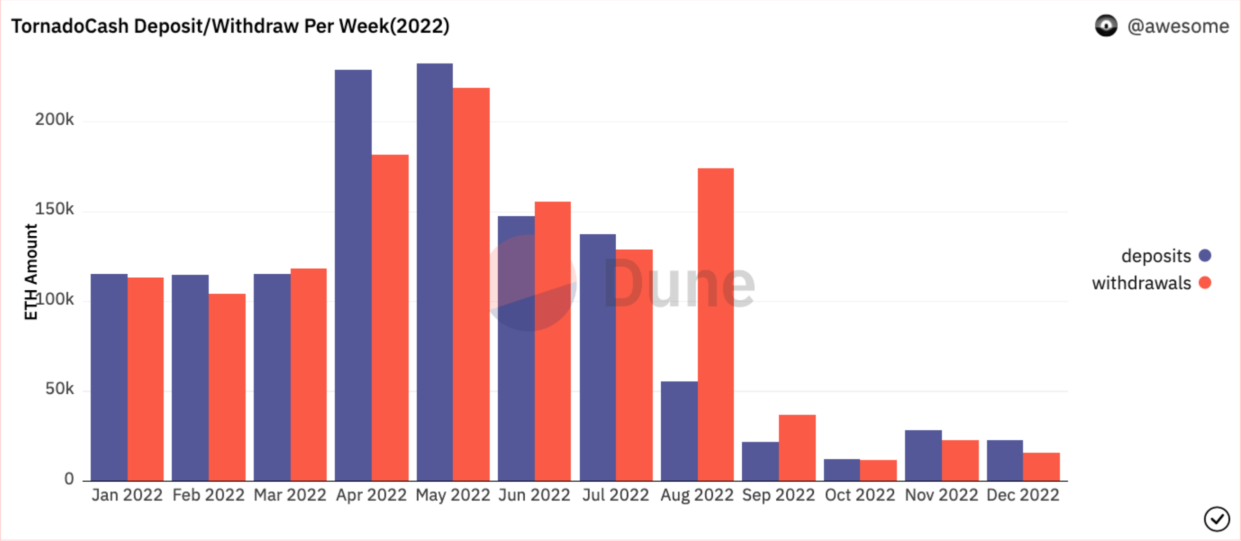
- On January 17, a small number of user accounts at Crypto.com were subject to unauthorized withdrawals.
- On February 8, the Gemini-hosted account of The IRA Financial was subject to a malicious withdrawal.
- On March 23, the Ronin Network cross-chain bridge hacking incident occurred, becoming one of the largest attacks in the cryptocurrency industry in terms of losses.

The LAZARUS GROUP has been identified as the perpetrator in a series of security incidents, and evidence suggests that they utilize systematic money laundering techniques as part of their operations:

- Initial stage: Convert all profits made on the ETH chain to ETH and then transfer the ETH in batches to either Tornado.Cash (for larger amounts) or a trading platform (for smaller amounts).
- Middle stage: Withdraw funds from Tornado.Cash in batches and exchange them for renBTC tokens. These tokens will then be transferred across to the BTC chain.
- Later stage: Withdraw funds from renBTC on the BTC chain, consolidate the funds, and then transfer them to a Coinjoin or mixer for further obfuscation.

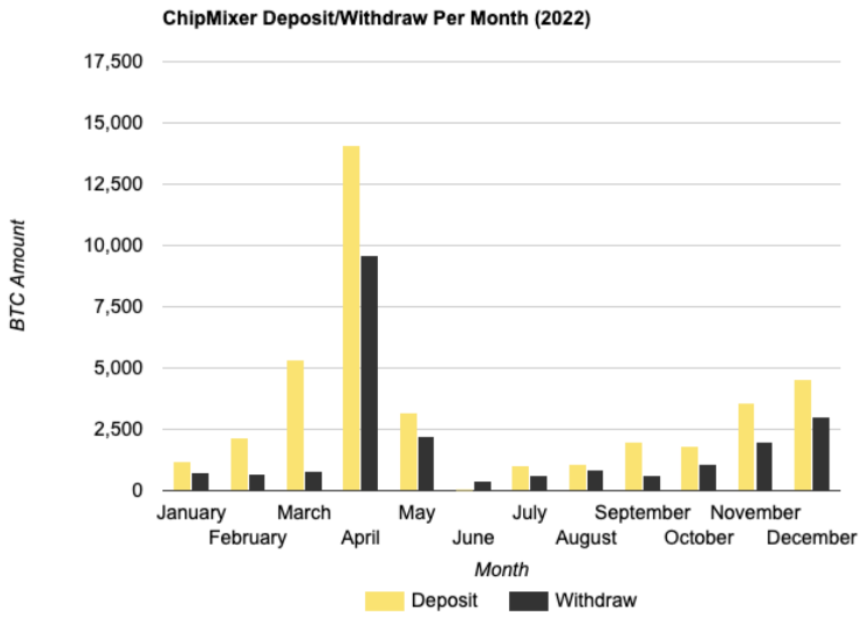
In the process of money laundering, it is common for hackers, black market groups, fraudsters, and Rug Pull project players to use various tools to help them launder money. Some of the most common tools used include Tornado.Cash on the ETH/BSC chain, Coinjoin tools on the BTC chain (such as ChipMixer), mixers (such as Blender and CryptoMixer), privacy wallets (such as Wasabi and Samourai, etc), currency swap platforms (like ChangeNOW, SimpleSwap, and FixedFloat), and other trading platforms.

The following is a summary of deposit and withdrawal data for some commonly used money laundering tools in 2022:



(Tornado.Cash Deposit/Withdrawals for 2022)

Tornado.Cash: In 2022, a total of 1,233,129 ETH (approximately $2.829 billion) was deposited by users to Tornado.Cash and a total of 1,283,186 ETH (approximately $2.837 billion) was withdrawn from Tornado.Cash.



(ChipMixer Deposit/Withdrawals for 2022)

ChipMixer: In 2022, users deposited a total of 40,065.33 BTC to ChipMixer and withdrew 22,582.44 BTC from ChipMixer.

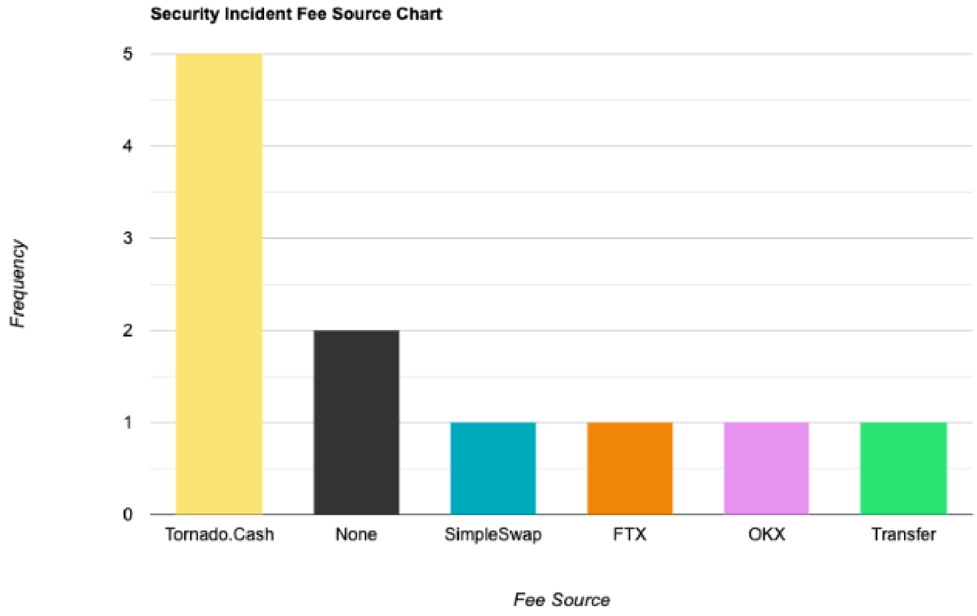
Blender: The LAZARUS GROUP was found to have used this mixer to launder stolen funds from the Ronin Network cross-chain bridge. As a result, the group was sanctioned by the US Department of the Treasury on May 6th, and the site is currently unavailable.

During the process of conducting an anti-money laundering analysis, it is essential to address two critical questions:

1. What is the origin of the funds used in the attack?
2. Where did the laundered funds ultimately end up?

To further illustrate these points, we will examine a number of key security incidents that took place in 2022.

What is the origin of the funds used in the attack?



(Funding Sources for Some Security Incidents)

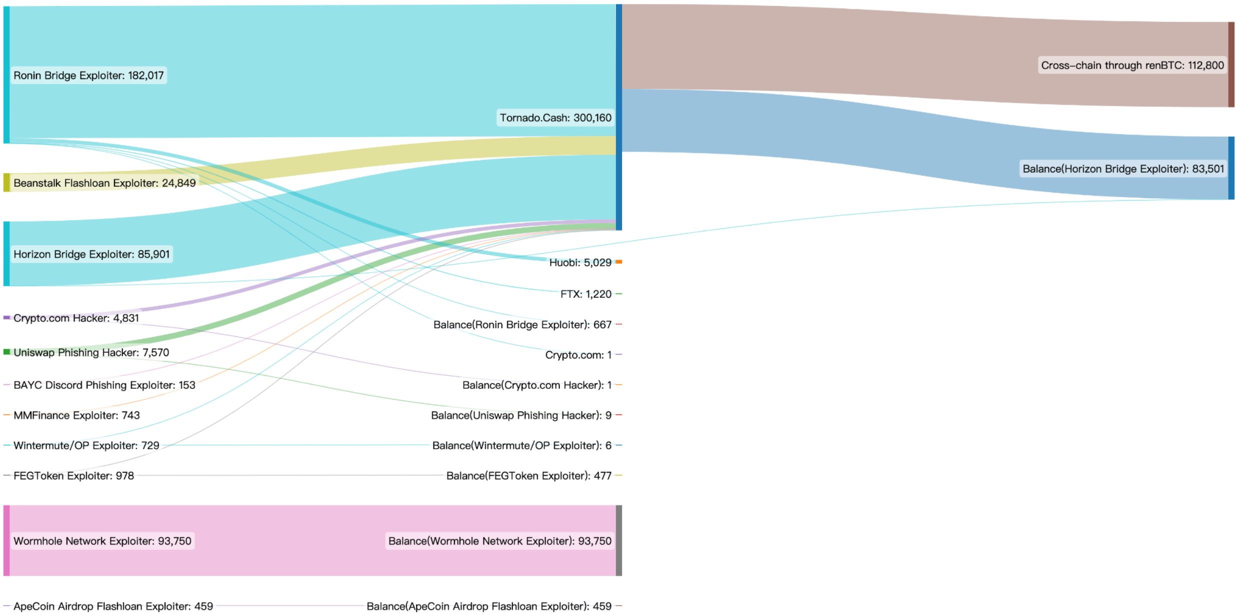
According to our analysis of the sources of funds used in some security incidents, most of the initial funding came from Tornado.Cash, as well as from currency exchange platforms, trading platforms, or transfers from other personal addresses.

Where did the laundered funds ultimately end up?

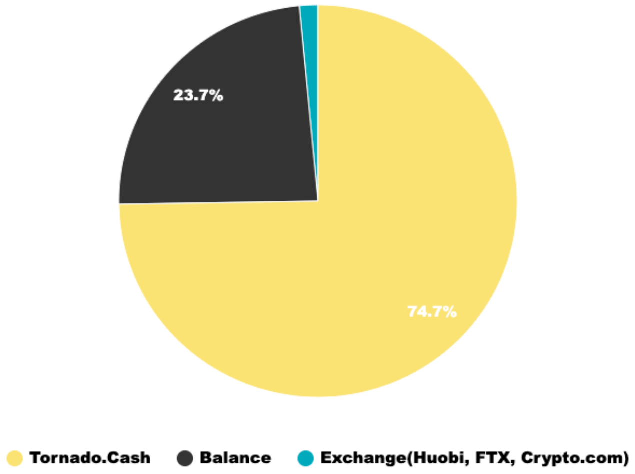
In terms of where the laundered money goes, our analysis of several security incidents in 2022 shows that the main process of money laundering takes place on the ETH or BTC chain. If the funds are not on these chains, hackers may also consider transferring them to these chains for further realization.

By analyzing the flow of some of the stolen ETH and BTC funds in 2022, we have created a diagram that outlines the flow of these funds. This has enabled us to make a preliminary assessment of the money laundering situation.

(1) ETH Money Laundering Flowchart



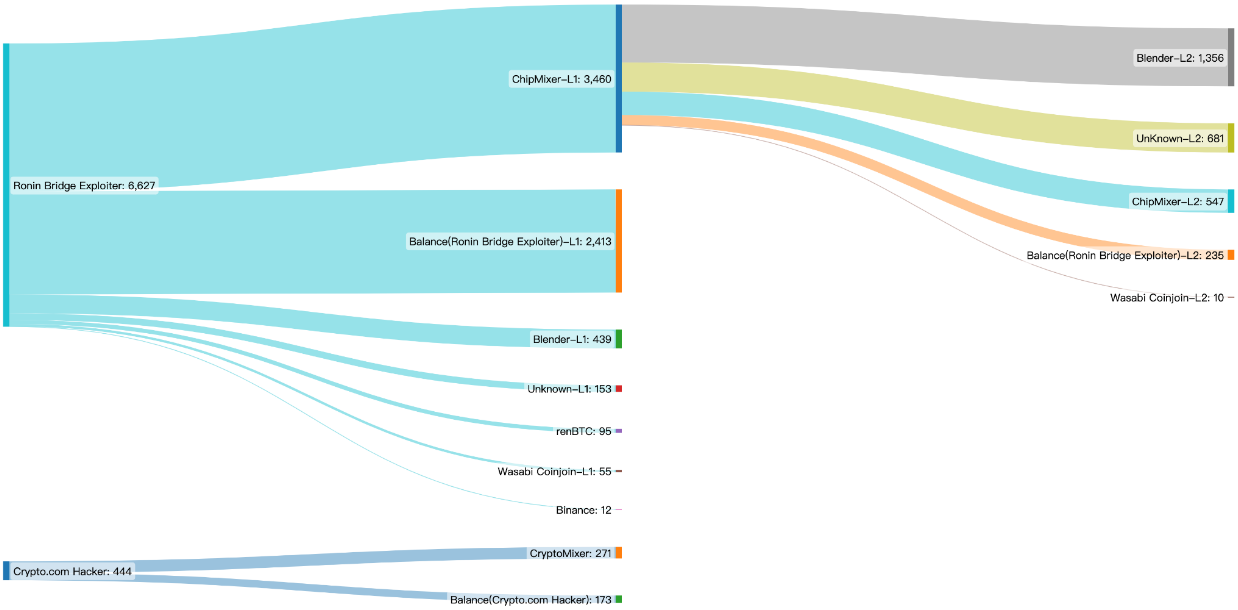
(ETH Fund Flow Chart of Some Security Incidents)



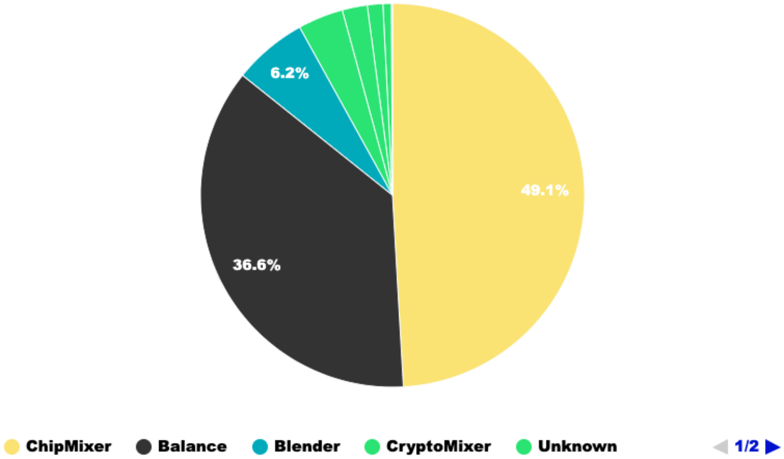
(Ratio of fund flow for ETH in some security incidents)

Based on our analysis of the flow of ETH funds in some security incidents, 74.6% of laundered funds were transferred to Tornado.Cash, with a total volume of 300,160 ETH. 23.7% of the laundered funds remained in the hacker's address and have not been transferred further, with a total volume of 95,570 ETH. The remaining 1.5% of laundered funds, or 6,250 ETH, were transferred to trading platforms.

(2) BTC Money Laundering Flowchart



(Flow of BTC funds in some security incidents)



(Ratios of fund flow for BTC in some security incidents)

According to our analysis of the flow of BTC funds in some security incidents, 48.9% of laundered funds were transferred to ChipMixer, totaling 3,460 BTC. 36.5% of laundered funds remained in the hacker's address and have not been transferred further, with a total volume of 2,586 BTC. The remaining laundered funds were transferred to various platforms: 6.2% to Blender, 3.8% to CryptoMixer, 2.1% to unknown entities, 1.3% to renBTC, 0.7% to Wasabi Coinjoin, and 0.1% to Binance trading platform.

II. Current State of Blockchain Security

2.1 Overview of Blockchain Security

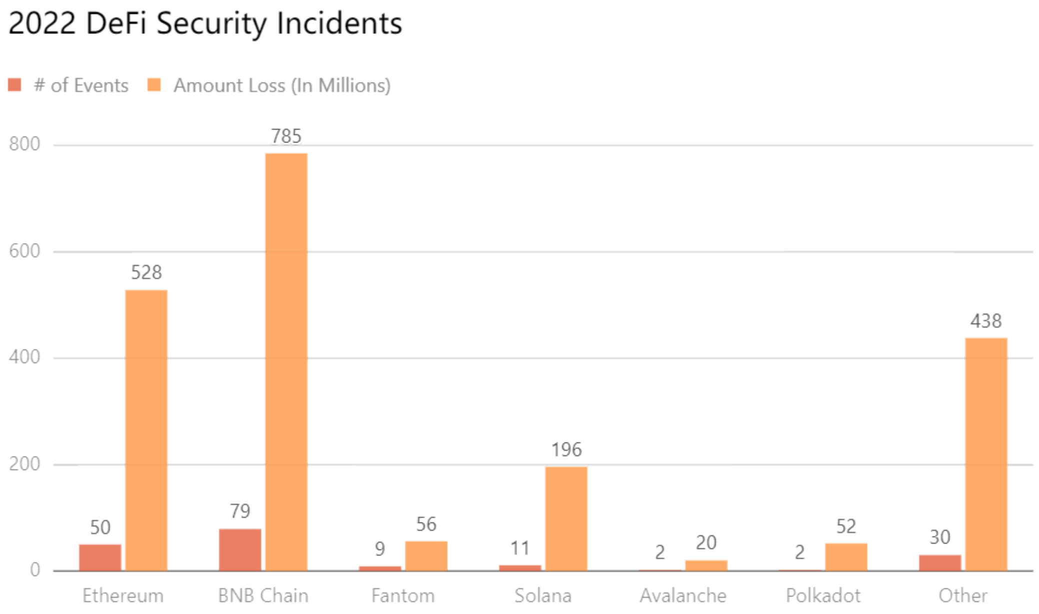
2.1.1 BlockChains

Blockchains are critical infrastructure in the Web3 space and are among the most competitive areas in the industry. However, on May 8, one of the most devastating crashes in cryptocurrency market history took place when the Terra network's stablecoin, UST, experienced a massive $285 million sell-off. This triggered a chain reaction that caused the price of Terra's native token, LUNA, to suddenly and unexpectedly plummet, resulting in a loss of nearly $40 billion in market value in a single day. The impact of this incident was so severe that it almost destroyed the entire ecosystem as we saw its TVL get reduced to near zero. This incident may even be seen as the trigger for the 2022 crypto winter.

2.1.2 DeFi / Cross-Chain Bridges

According to DeFi Llama, the total value locked in DeFi was approximately $39.8 billion at the end of December, representing a massive 75% drop year-over-year. Ethereum dominates with 58.5% of the total DeFi TVL, or around $23.3 billion, followed by TRON with $4.3 billion and BNB Chain with $4.2 billion. Interestingly, Ethereum's share of the DeFi TVL decreased by 35% in May 2022, while TRON's share increased by 47%.

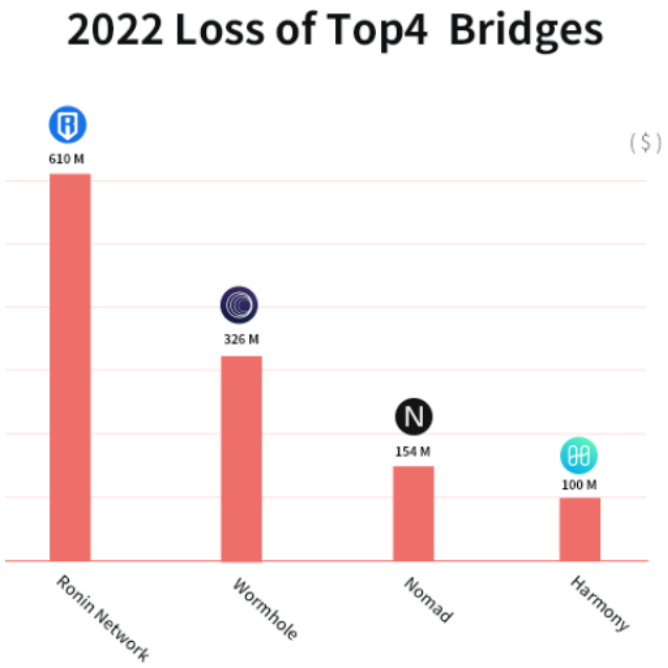
According to SlowMist Hacked, there were 183 major DeFi security incidents in 2022, resulting in losses of $2.075 billion, or approximately 55% of the total losses for the year. Among these incidents, there were approximately 79 on BNB Chain, resulting in a total loss of around $785 million, making it the platform with the highest losses. Ethereum had around 50 security incidents, resulting in a total loss of about $528 million, followed by Solana with about 11 incidents and a total loss of around $196 million.



(Distribution of DeFi security incidents in 2022)

Cross-chain bridges allow users to transfer crypto assets from one blockchain to another, mainly addressing the issue of multi-chain scalability. According to Dune Analytics, the total locked-in value (TVL) of Ethereum cross-chain bridges is around $8.39 billion, a decrease of about 31% from the first half of the year. The highest TVL is currently held by Polygon Bridges ($3 billion), followed by Arbitrum Bridges ($1.28 billion) and Optimism Bridges ($850 million). Due to the high volume of funds present in cross-chain bridge smart contracts, coupled with a lack of security audits, these systems have become targets for malicious hackers.

According to SlowMist Hacked, there were 16 major cross-chain security incidents in 2022, resulting in losses of $1.212 billion, or approximately 32% of total losses for the year. In 2022, there will be a total of 10 security incidents that cost hundreds of millions of dollars, of which cross-chain bridges account for 4, most of which are caused by the leakage of private keys.



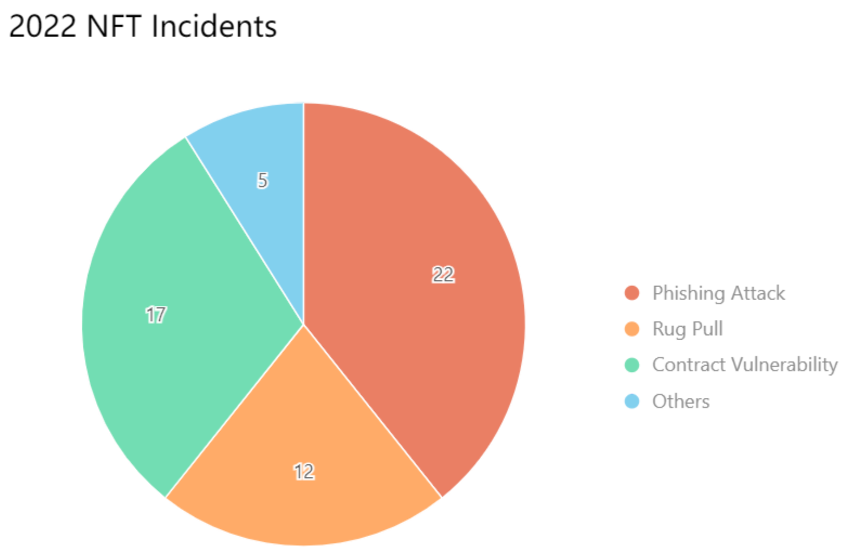
(Losses Top4 on cross-chain bridges in 2022)

In conclusion, in order to eliminate vulnerabilities and reduce security risks as much as possible, projects must make a concerted effort to conduct a comprehensive and thorough security audit of their project before it goes live. At the same time, it is recommended that each project party increase its asset protection efforts by implementing a multi-signature mechanism. On the other hand, projects must have a deep understanding of the architecture of the protocols they are using and the architectural design of their own project when interacting with other protocols or forking code from other protocols, in order to ensure compatibility between protocols and prevent further losses. It is crucial for users to thoroughly research projects before investing in them, especially as the blockchain space becomes more diverse. This includes verifying that the project is open source and has undergone an audit. Additionally, it is important for users to remain aware of potential risks when participating in any project. By taking these precautions, users can protect themselves from potential losses.

2.1.3 NFT

According to NFTScan, NFTs experienced significant growth in 2022, with a total of 198 million transactions on Ethereum by the end of December, far exceeding the numbers for 2020 and 2021. The number of NFT transactions on BNBChain reached 345 million for the year, while the number on Polygon reached 793 million for the year.

According to SlowMist Hacked, which may not represent the full scope of NFT track security incidents in 2022, there were approximately 56 such incidents reported, resulting in losses totaling over $65.44 million. Many of these incidents were caused by phishing attacks, accounting for about 39% (22 incidents), followed by Rug Pulls, accounting for about 21% (12 incidents). The remaining 30% (17 incidents) were caused by contract vulnerabilities or other internal factors.



(Distribution of causes for NFT security incident losses in 2022)

2.1.4 Wallets / Exchanges

On February 8, the U.S. Department of Justice announced that it had seized $3.6 billion worth of bitcoin in connection with the 2016 hack of cryptocurrency exchange Bitfinex. 34-year-old Ilya Lichtenstein and her 31-year-old wife Heather Morgan were arrested in New York and charged with conspiracy to commit money laundering and fraud. This was the largest financial seizure ever by the U.S. Department of Justice.

On November 6, CZ, the founder of Cryptocurrency, tweeted about his decision to liquidate all remaining FTT on his books, leading to a standoff between the two exchanges. Despite attempts by Alameda CEO and FTX CEO SBF to reassure users and contradict the negative news, this triggered a rapid bankruptcy of FTX after liquidity dried up. Ultimately, FTX crashed and SBF was arrested. The lack of transparency at centralized exchanges has caused a crisis of confidence, and the lack of regulatory oversight has become more evident. Whether it's stronger protections for consumers or clearer rules for institutions, regulatory changes will become increasingly apparent.

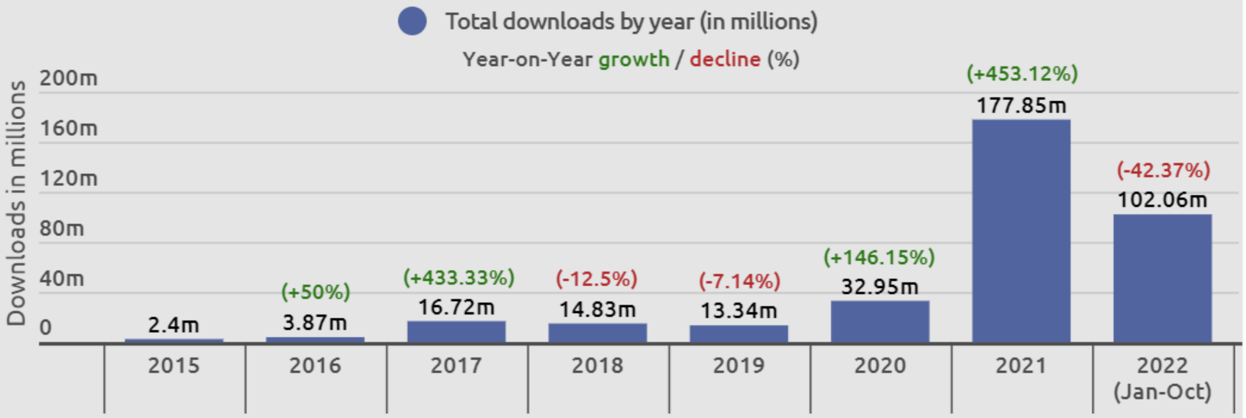
In the aftermath of the FTX collapse, sales of hardware wallets have surged, with MetaMask, the wallet with the most users, reaching 30 million monthly active users. According to Finbold data, based on the top 21 cryptocurrency storage apps, there have been approximately 102.06 million downloads of crypto wallets on Android and iOS devices between January 2022 and October 2022. While this number is lower than the 177.85 million downloads during the 2021 bull market, it is higher than any other year except for 2021. A breakdown by month shows that crypto wallet downloads started the year on a downward trend, but increased significantly after the Terra/Luna crash and the FTX meltdown.

Crypto Wallet App Downloads Worldwide* (2015-2022)

(from January 2015 to October 2022)

Details: Estimated number of downloads of the 21 largest apps that allow for cryptocurrency storage worldwide from January 2015 to October 2022. The numbers provided are estimates based on wallets available worldwide, and may not necessarily include wallets that are popular in a specific country. The data presented include download figures for both Android and iOS devices.

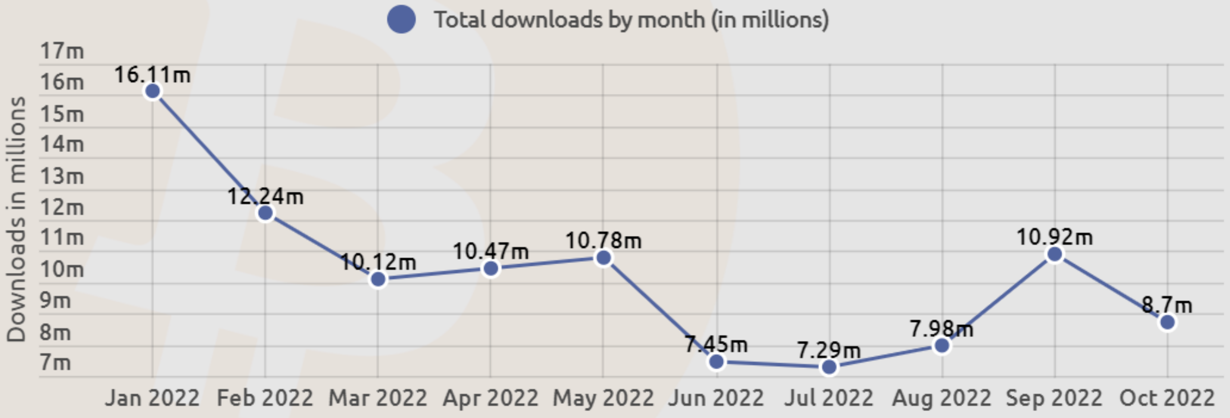
Sources: Statista, Finbold, AppMagic



***Supplementary note:** The following apps include in the list: ABNB Coin Wallet; Binance; Bitcoin & Crypto DeFi Wallet; Bitcoin Wallet; Blockchain.com Wallet; BRD Bitcoin Wallet; BTC Coin Wallet; Coinbase; Coinbase Wallet; Coinomi; CoinSwitch; Crypto.com l DeFi Wallet; Dogecoin Wallet; Enjin Wallet; Exodus Wallet; MetaMask Wallet; Satoshi Wallet; Status Wallet; Sweat Wallet; Trust Wallet; Wirex Wallet.

Crypto Wallet App Downloads Worldwide in 2022 (by Month)

Details: Estimated number of downloads of the 21 largest apps that allow for cryptocurrency storage worldwide from January 2022 to October 2022. The numbers provided are estimates based on wallets available worldwide, and may not necessarily include wallets that are popular in a specific country. The data presented include download figures for both Android and iOS devices.



2.1.5 Others

The irreversibility and anonymity of blockchain technology effectively protects privacy, but also provides cover for cybercrime. As the concepts of metaverses and NFTs have gained popularity, there have been periodic instances of cryptocurrency theft and fraud, with many unscrupulous actors issuing so-called virtual assets under the banner of blockchain in order to commit fraud.

According to data from the Payment and Settlement Department of the People's Bank of China, in 2021, payments using cryptocurrencies ranked second only to bank transfers in terms of payment methods involving fraudulent amounts, reaching a high of $750 million. In contrast, in 2020 and 2019, this number was only $130 million and $30 million, respectively, showing a clear trend of significant yearly growth. Notably, cryptocurrency transfers are increasingly being used in "piggyback" scams, with $139 million of "piggyback" scam funds paid in cryptocurrency in 2021, 5 times more than in 2020 and 25 times more than in 2019.

According to a report released by the Federal Trade Commission (FTC), more than 46,000 people have reported experiencing cryptocurrency scams in over a year starting in 2021, with losses totaling over $1 billion. The FTC Consumer Sentinel Network's fraud report states that the most common type of cryptocurrency scam is investment-related fraud, accounting for $575 million of the $1 billion total. The most common cryptocurrencies paid to scammers include BTC (70%), USDT (10%), and ETH (9%).

To avoid risks, individual users should adhere to the following security rules and principles.

Two major security rules:

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

Security principles:

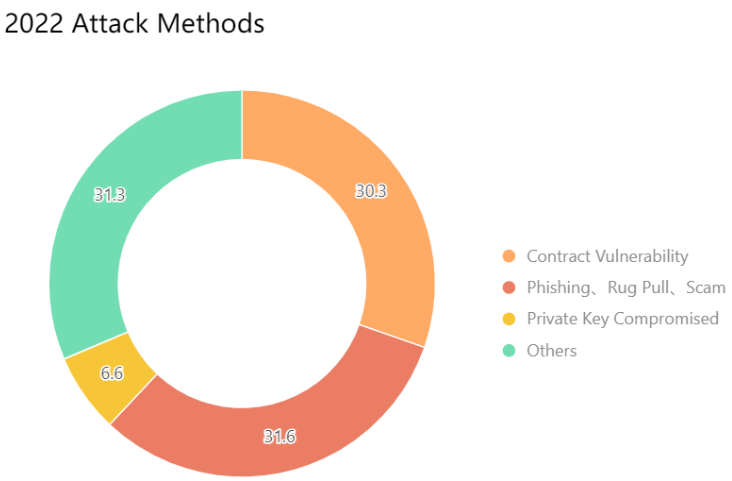
- When seeking knowledge on the internet, it is important to refer to at least two sources for everything, in order to ensure that you are getting a well-rounded and accurate understanding of the topic. It is also essential to corroborate the information from these sources, by checking that they agree with each other and align with other known facts. Even when the information comes from seemingly reliable sources, it is important to always remain skeptical and to verify everything for yourself. By following these steps, you can avoid being swayed by biased or misleading information and make more informed decisions.
- One way to protect yourself from risk is with diversification. This means not putting all of your eggs in one basket, and instead spreading out your investments, resources, or efforts across multiple areas or options. By diversifying, you can reduce the impact of any one potential failure or loss, and increase the overall stability and security of your situation.
- When it comes to wallets that hold important assets, it is generally advisable to be cautious about updating them. While updates may offer new features or improvements, they can also introduce new vulnerabilities or compatibility issues. Therefore, it is often best to only update these wallets when necessary, in order to get the benefits of the update while minimizing the potential risks. This might mean waiting for critical security patches or stability fixes, rather than updating to the latest version as soon as it is released. By following this approach, you can help ensure the safety and security of your assets, while still being able to take advantage of new features and improvements as needed.
- One key principle to follow when it comes to digital transactions is "what you see is what you sign." This means that when you are presented with something to sign or approve, you should carefully review and verify what you are being asked to sign, and make sure that it aligns with your expectations and intentions. It is important to pay attention to the details and to understand the implications of what you are agreeing to. Additionally, once you have signed or approved something, you should expect the resulting outcome to match your expectations and not be surprised afterward. By following this principle, you can protect yourself from errors or misunderstandings, and ensure that your digital interactions are conducted in a clear and transparent manner.

- Maintaining the security of your digital systems is an ongoing process, and one of the key ways to do this is by keeping up with system updates. These updates often include critical security patches and other enhancements that can help protect your systems from vulnerabilities or threats. Therefore, it is important to pay attention to system security updates and to act on them as soon as they are available. This might involve setting your systems to update automatically, or proactively checking for and installing updates on a regular basis. By staying current with system updates, you can help ensure that your systems are as secure as possible and are less likely to be compromised.
- Don't download & install programs recklessly can actually prevent most risks.

As you navigate the digital landscape, it is important to be aware of the potential risks and challenges that you may encounter. One helpful resource that you may want to consider is the "Blockchain dark forest selfguard handbook" This handbook provides practical guidance and advice for staying safe and secure in the online world and covers a range of topics including cyber threats, phishing scams, and the importance of maintaining good online habits. By reading and familiarizing yourself with the content of this manual, you can gain a better understanding of how to protect yourself and your assets online and make informed decisions about how to stay safe in the digital world.

2.2 Attack Methods

In the 303 security incidents that occurred, the attack techniques can be broadly categorized into three types: those that were caused by design flaws or vulnerabilities within the project itself, those that used techniques such as rug pull, phishing, or scams, and those that resulted in asset loss due to private key leakage.



(Attack Methods in 2022)

In 2022, the majority of attacks on projects were due to flaws in the design of the program itself or vulnerabilities in contracts. These attacks resulted in a total of 92 incidents, costing nearly $1.1 billion in losses. The most frequently occurring type of attack was caused by flash loan attacks, with 33 attacks leading to $348 million in losses. Other attack types included problems with re-entry, price manipulation, and validation issues.

Private key theft occurred only 6.6 percent of the time, resulting in $762 million in losses. The biggest losses from private key theft were the Ronin and Harmony incidents, which were both related to cross-chain bridges.

Users in the Web3 world often have varying levels of security awareness, which has led to numerous phishing attacks. Attackers have been known to take over official media platforms like Discord and Twitter for various projects. This is so they can impersonate official media accounts and post phishing Mint and AirDrop links, sometimes alongside real official content in order to confuse the public. They may also use search engine ads to promote fake websites or domain names that are similar to official ones, send fake emails with attractive giveaways, or provide fake app download links using information about new users. It is crucial for users to raise their security awareness and, if you do fall victim to such an attack, transfer your assets as soon as possible, stop the loss in time, retain evidence, and seek help from security agencies in the industry if necessary.

Another type of attack is the Rug Pull, where a developer abandons a project and takes the funds with them, usually on purpose. This can happen in various ways, such as when a developer provides initial liquidity to push up the price of a project and then withdraws that liquidity. The developer may create a crypto project, attract users to invest in it through marketing techniques, and then suddenly steal the invested funds, sell off the crypto assets, and disappear, leaving users with significant losses. Another example is a website that attracts thousands of deposits and then shuts down. In 2022, there were 51 Rug Pull incidents, resulting in approximately $188 million in losses, often in the BSC ecosystem and NFT space.

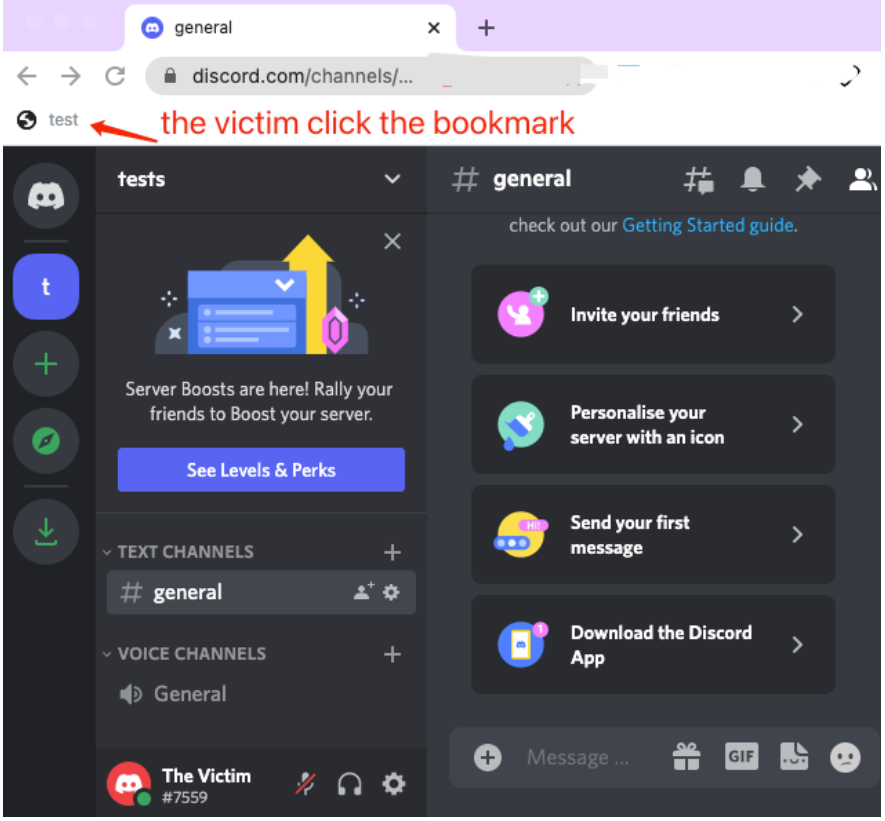
We also saw new attack techniques being used in 2022, this included front-end malicious attacks, DNS attacks, and BGP hijacking. One of the most unusual types of attacks was the loss of assets due to manmade configuration errors.

2.3 Phishing/Scam Methods

This section only outlines a selection of phishing and scamming techniques that SlowMist has publicly disclosed in 2022.

2.3.1 Use of Malicious browser Bookmark to steal Discord Token

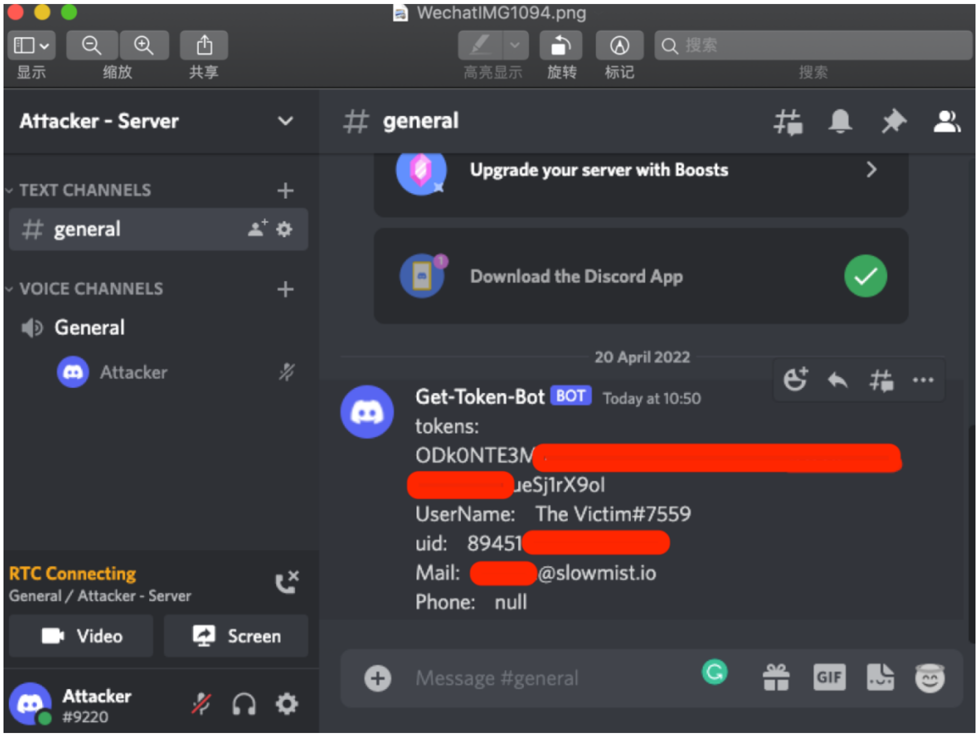
It is a concerning issue that bookmark managers, a feature included in modern browsers for user convenience, can be vulnerable to exploitation by attackers through the use of malicious phishing pages. By inserting JavaScript code into bookmarks through these phishing pages, attackers can potentially gain access to a Discord user's information and take over the permissions of a project owner's account. When a Discord user clicks on a malicious bookmark, the JavaScript code is executed in their Discord domain, allowing the attacker to steal the Discord Token. With this token, the attacker can then access the project owner's Discord account and conduct actions such as creating a Discord webhook bot and posting fake messages for phishing purposes. It is important for users to be cautious when interacting with unfamiliar bookmarks to protect against these types of attacks.



the victim click the bookmark

(Malicious bookmark phishing demo picture)

The following demonstrates how an attacker can use JavaScript code to obtain personal information, such as a Discord Token, and send it through a Discord Server's webhook:



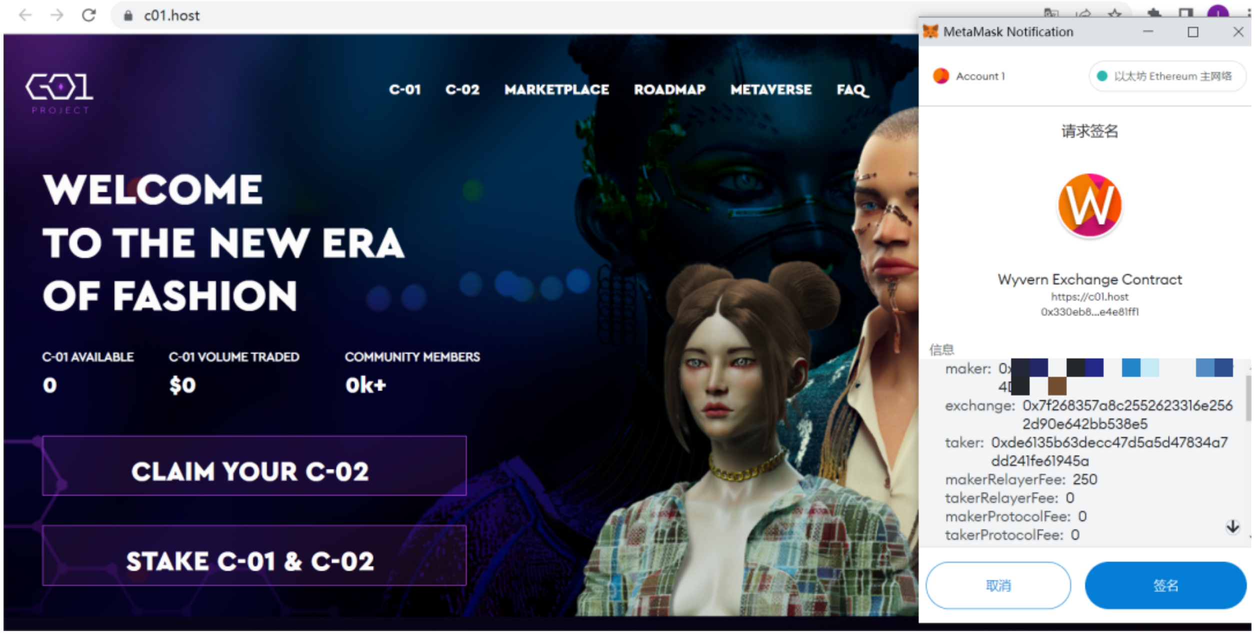
Get-Token-Bot BOT Today at 10:50
tokens:
ODkONTE3M[redacted]
[redacted]ueSj1rX9ol
UserName: The Victim#7559
uid: 89451[redacted]
Mail: [redacted]@slowmist.io
Phone: null

(Malicious bookmark phishing demo picture)

As demonstrated, an attacker can use a malicious bookmark to gain access to a victim's personal information, such as their Discord Token, when the victim is logged into Discord on the web. By guiding the victim to add the malicious bookmark through a phishing page and then tricking them into clicking on it while they are logged in to Discord on the web, the attacker can trigger the malicious code and send the victim's personal information to their own Discord channel through a webhook set up by the attacker. It is important to be aware of these types of attacks and take steps to protect your personal information.

2.3.2 “Zero Dollar Purchase” NFT Phishing

Let’s first examine the signature content of this phishing site:
Maker: User address
Taker: 0xde6135b63decc47d5a5d47834a7dd241fe61945a
Exchange: 0x7f268357A8c2552623316e2562D90e642bB538E5 (OpenSea V2 Contract)



请求签名

Wyvern Exchange Contract
https://c01.host
0x330eb8...e4e81ff1

信息

```
maker: 0x[redacted]
exchange: 0x7f268357a8c2552623316e256
          2d90e642bb538e5
taker: 0xde6135b63decc47d5a5d47834a7
       dd241fe61945a
makerRelayerFee: 250
takerRelayerFee: 0
makerProtocolFee: 0
takerProtocolFee: 0
```

("Zero Dollar Purchase" Phishing Demo Image)

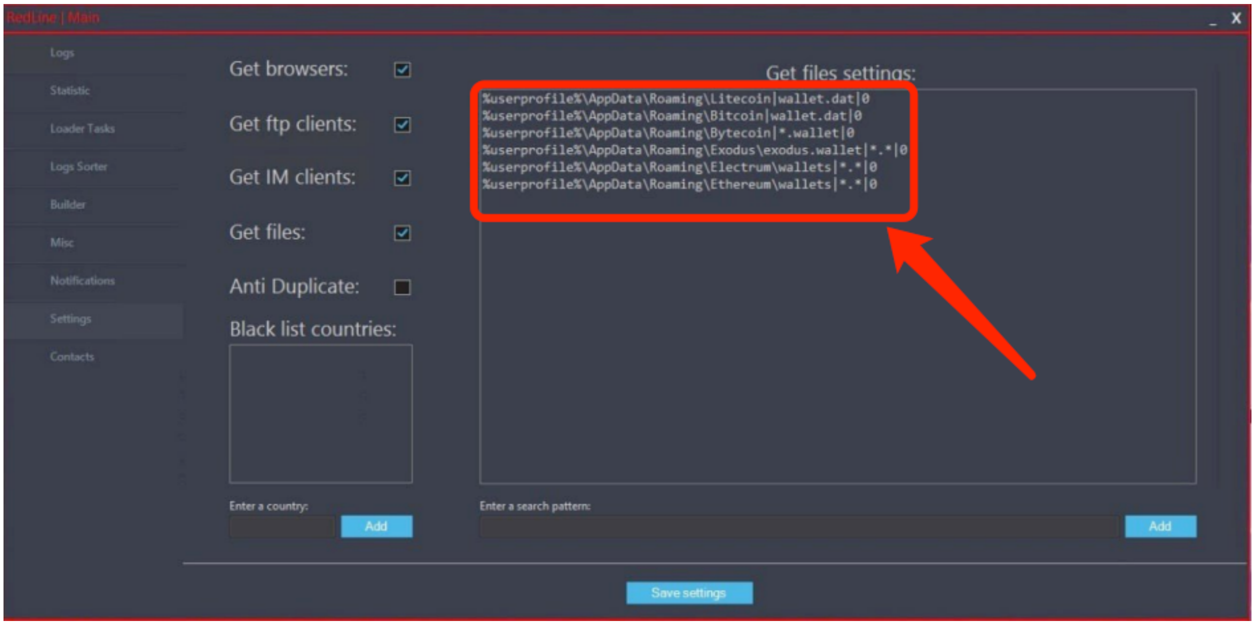
This common type of NFT phishing involves scammers tricking users into signing over their NFTs for 0 ETH (or any token). The scammer creates a sales order that appears legitimate to the user, but once the user signs the order, the scammer can then purchase the user's NFTs through OpenSea at a price determined by the scammer, effectively allowing them to "buy" the NFTs without spending any money. It is important to be cautious when buying and selling NFTs and to verify the authenticity of any sales orders to protect against these types of scams.

Unfortunately, it’s not possible to deauthorize a stolen signature through sites like Revoke.Cash or Etherscan, which leaves it vulnerable to use by an attacker. However, you can deauthorize any previous pending orders that you had set up, which can help mitigate the risk of phishing attacks and prevent the attacker from using your signature.

2.3.3 Redline Stealer Trojan Horse Currency Theft

Beware of phishing attacks that may try to trick you into sharing your cryptocurrency information. These attacks often occur through private messages on Discord, where someone may invite you to participate in the internal testing of a new game project, claiming to offer discounts. They may also send you a program to download, usually in the form of a compressed file that contains an executable file of about 800 MB. If you run this file on your computer, it will scan for files that contain keywords like 'wallet' and upload them to the attacker's server, compromising your cryptocurrency security.

RedLine Stealer is a malicious Trojan that was first discovered in March 2020. It is sold on underground forums and is designed to steal information such as saved credentials, autocomplete data, and credit card information from a browser. When it is run on a target machine, it collects details such as usernames, location data, hardware configuration, and installed security software. The latest version of RedLine Stealer also has the ability to steal cryptocurrency, scanning for installed digital currency wallet information on the local computer and uploading it to a remote control machine. In addition to stealing cryptocurrency, RedLine Stealer can also upload and download files, execute commands, and send back periodic information about the infected computer. It is known to specifically scan for cryptocurrency wallet directories and wallet files.



Get browsers: ☑

Get ftp clients: ☑

Get IM clients: ☑

Get files: ☑

Anti Duplicate: □

Black list countries:

Get files settings:

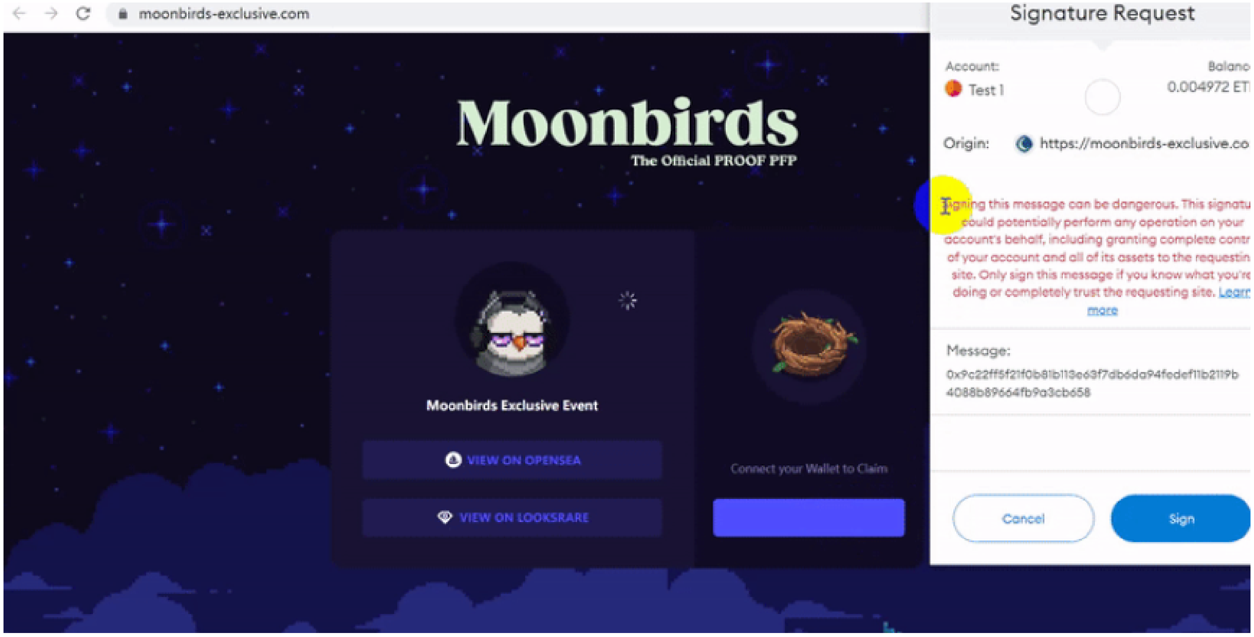
```
%userprofile%\AppData\Roaming\Litecoin|wallet.dat|0
%userprofile%\AppData\Roaming\Bitcoin|wallet.dat|0
%userprofile%\AppData\Roaming\Bytecoin|*.wallet|0
%userprofile%\AppData\Roaming\Exodus\exodus.wallet|*.*|0
%userprofile%\AppData\Roaming\Electrum\wallets|*.*|0
%userprofile%\AppData\Roaming\Ethereum\wallets|*.*|0
```

(RedLine Stealer Trojan Coin Stealer Demo Image)

2.3.4 “Blank Check” eth_sign Phishing

Beware of phishing attacks that use the eth_sign method to trick you into signing transactions. When you connect your wallet and click 'Claim,' a signature application box may pop up with a red warning from MetaMask. It may be difficult to tell from this window exactly what you are being asked to sign. This type of signature, known as an Ethereum 'blank check,' allows scammers to use your private key to sign any transaction they choose.

The eth_sign method can sign any hash, so it can be used to sign our signed bytes32 data. This means that once an attacker obtains your address and connects to the DApp, they can construct any data (such as a native token transfer or contract call) and ask you to sign it through eth_sign.



Signature Request

Account: Test 1

Balanc 0.004972 ET

Origin: https://moonbirds-exclusive.co

Signing this message can be dangerous. This signatu could potentially perform any operation on your account's behalf, including granting complete contr of your account and all of its assets to the requestin site. Only sign this message if you know what you're doing or completely trust the requesting site. Learn more

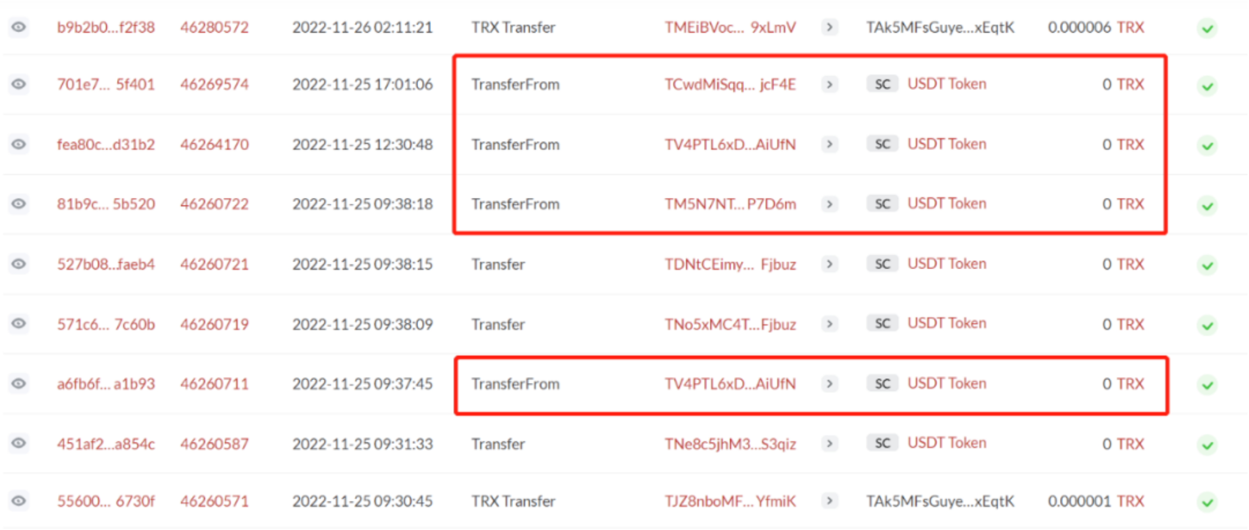
Message:
0x9c22ff5f21f0b81b113e63f7db6da94fedef11b2119b4088b89664fb9a3cb658

(eth_sign Phishing Demo Image)

This type of phishing can be very confusing, especially when it comes to authorization. In the past, we've seen attackers use MetaMask's eth_sign method to get users to sign a hash of bytes32 without giving them a visual representation of the data. This can make it difficult for the user to understand what they're signing and whether or not it's safe.

2.3.5 Same Ending Number + TransferFrom Zero Transfer Scam

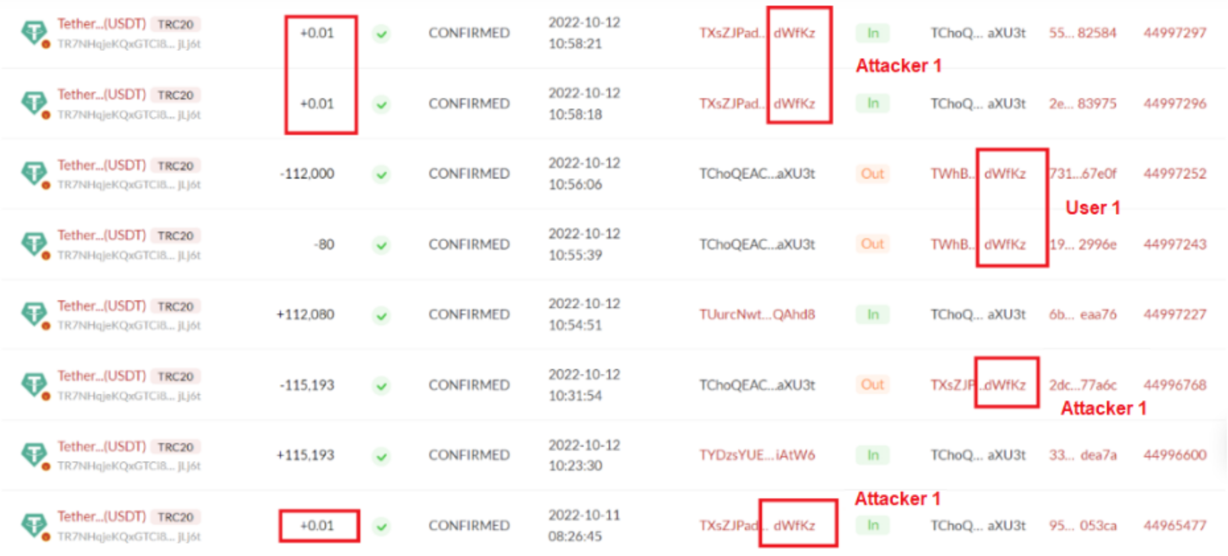
It appears that the user's address has been showing a lot of 0 USDT transfers from unknown addresses in their transfer history. Upon investigation, we discovered that these transactions are being done by calling the TransferFrom function. The issue is that the TransferFrom function of the token contract does not require the authorized transfer amount to be greater than 0, so it's possible for a malicious attacker to initiate a transfer of 0 from any user's account to an unauthorized account without the transaction failing. This means that the attacker can take advantage of this condition to continuously initiate TransferFrom operations against active users on the chain, triggering transfer events and potentially causing confusion or alarm for the affected users.



	b9b2b0...f2f38	46280572	2022-11-26 02:11:21	TRX Transfer	TMEiBVoc... 9xLmV	›	TAk5MFsGuye...xEqtK	0.000006 TRX	✓
	701e7... 5f401	46269574	2022-11-25 17:01:06	TransferFrom	TCwdMiSqq... jcF4E	›	SC USDT Token	0 TRX	✓
	fea80c...d31b2	46264170	2022-11-25 12:30:48	TransferFrom	TV4PTL6xD...AiUfN	›	SC USDT Token	0 TRX	✓
	81b9c... 5b520	46260722	2022-11-25 09:38:18	TransferFrom	TM5N7NT... P7D6m	›	SC USDT Token	0 TRX	✓
	527b08...faeb4	46260721	2022-11-25 09:38:15	Transfer	TDNtCEimy... Fjbuz	›	SC USDT Token	0 TRX	✓
	571c6... 7c60b	46260719	2022-11-25 09:38:09	Transfer	TNo5xMC4T...Fjbuz	›	SC USDT Token	0 TRX	✓
	a6fb6f... a1b93	46260711	2022-11-25 09:37:45	TransferFrom	TV4PTL6xD...AiUfN	›	SC USDT Token	0 TRX	✓
	451af2...a854c	46260587	2022-11-25 09:31:33	Transfer	TNe8c5jhM3...S3qiz	›	SC USDT Token	0 TRX	✓
	55600... 6730f	46260571	2022-11-25 09:30:45	TRX Transfer	TJZ8nboMF... YfmiK	›	TAk5MFsGuye...xEqtK	0.000001 TRX	✓

(TransferFrom Transactions Demo Diagram)

In addition to the ongoing issue of 0 USDT transfer harassment, we have also noticed that attackers are constantly airdropping small amounts of tokens (such as 0.01 USDT or 0.001 USDT) to users with larger and more frequent transactions. These airdrops often have the end number of the attacker's address being similar to the end number of the user's address, usually the last few digits, in an attempt to trick users into accidentally copying the wrong address in their transfer history. This can lead to the loss of assets if the user is not careful.



Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	+0.01	✓	CONFIRMED	2022-10-12 10:58:21	TXsZJPad... dWfKz	In	TChoQ... aXU3t	55... 82584	44997297
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	+0.01	✓	CONFIRMED	2022-10-12 10:58:18	TXsZJPad... dWfKz	In	TChoQ... aXU3t	2e... 83975	44997296
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	-112,000	✓	CONFIRMED	2022-10-12 10:56:06	TChoQEAC...aXU3t	Out	TWhB... dWfKz	731...67e0f	44997252
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	-80	✓	CONFIRMED	2022-10-12 10:55:39	TChoQEAC...aXU3t	Out	TWhB... dWfKz	19... 2996e	44997243
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	+112,080	✓	CONFIRMED	2022-10-12 10:54:51	TUurcNwt...QAhd8	In	TChoQ... aXU3t	6b... eaa76	44997227
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	-115,193	✓	CONFIRMED	2022-10-12 10:31:54	TChoQEAC...aXU3t	Out	TXsZJP...dWfKz	2dc...77a6c	44996768
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	+115,193	✓	CONFIRMED	2022-10-12 10:23:30	TYDzsYUE...iAtW6	In	TChoQ... aXU3t	33... dea7a	44996600
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jLj6t	+0.01	✓	CONFIRMED	2022-10-11 08:26:45	TXsZJPad... dWfKz	In	TChoQ... aXU3t	95... 053ca	44965477

(Same End Number Phishing Demo Diagram)

As we've seen in subsections 2.2 and 2.3, there are many different attack techniques and scenarios that hackers use. The reality is that the world of cybersecurity is constantly evolving, and hackers are always finding new ways to attack. The best we can do is to stay vigilant and continue improving our knowledge and understanding of these threats in order to protect ourselves and our assets. It's important to stay up-to-date on the latest attack methods and to be proactive in implementing security measures to prevent ourselves from becoming victims.

2.4 Top 10 Security Incident Losses

In this section, we'll be covering the top 10 security incidents with the most losses in 2022.

2.4.1 Ronin Network Losses Exceed $610 Million

On March 29th, the Ronin Network, a sidechain of Axie Infinity, issued a community alert regarding a security breach that resulted in the theft of 173,600 ETH and 25.5 million USDC, worth over $610 million. The hack occurred on March 23rd, but was not discovered until users reported being unable to withdraw 5k ETH from the bridge. The attackers used a hacked private key to forge withdrawals and siphon off funds from the Ronin bridge in just two transactions. This incident resulted in a greater loss than the PolyNetwork hack from the previous year, which also saw the theft of over $600 million.

According to authorities, the North Korean hacking group LAZARUS GROUP is believed to be responsible for the attack. The breach was made possible due to a whitelist process that was put in place in November, when Sky Mavis requested assistance from Axie DAO in distributing free transactions. The high volume of users led Axie DAO to whitelist Sky Mavis and allow them to sign various deals on its behalf, a process that was halted in December. However, access to the whitelist was not revoked, which allowed an attacker to sign from the Axie DAO verifier via gas-free RPC after gaining access to the Sky Mavis system. Sky Mavis' Ronin chain consists of nine verification nodes, and at least five signatures are required to identify a deposit or withdrawal event. The attackers were able to find a backdoor through the gas-free RPC node and eventually took control of five private keys, including four of Sky Mavis' Ronin verifiers and one run by a third party, Axie DAO.

2.4.2 BNBChain Vulnerability Exploit

On October 7th, the BNB Chain cross-chain bridge, BSC Token Hub, was attacked. The hackers were able to capture a total of 2 million BNBs, worth over $570 million, in two separate attacks by exploiting a vulnerability in the cross-chain bridge. According to a tweet by security researcher Samczsun, the root cause of the attack was the attackers' ability to forge proofs for specific blocks. This incident serves as a reminder of the importance of securing all aspects of our systems and the potential consequences of neglecting to do so.

2.4.3 Wormhole's Loses Over $300 Million

On February 3rd, there was a security incident on the Wormhole network in which attackers exploited a signature verification vulnerability to mint 120,000 WETH on Solana, resulting in a loss of over $326 million. Wormhole released a report on the incident, explaining that the vulnerability in question was an error in the signature verification code of the core Wormhole contract on the Solana side, which allowed the attackers to forge messages from the "guardian" and mint WETH. This was the largest loss scale incident in a hacking attack on Solana to date and serves as a reminder of the importance of thoroughly checking and testing the security of our systems.

2.4.4 Beanstalk Farms Attacked by Flash Loans and Proposals

On April 17th, Beanstalk Farms, an algorithmic stablecoin project based on Ethereum, was attacked, resulting in a loss of approximately $182 million. The attack was made possible due to a lack of a time interval between the two stages of voting and proposal execution, allowing the attacker to directly execute a malicious proposal without community review after the voting process was completed. Interestingly, the attackers donated $250,000 of the stolen funds to an address used to raise donations for the Ukrainian government. This incident serves as a reminder of the importance of implementing proper safeguards and review processes to prevent unauthorized actions.

2.4.5 Wintermute Loses $160 million

On September 20th, Evgeny Gaevoy, the founder and CEO of crypto market maker Wintermute, tweeted that Wintermute had lost $160 million in a DeFi hack. Wintermute had used Profanity to create a wallet in order to optimize handling fees, but later discovered that Profanity had a loophole. While attempting to transfer funds from the old address to a new one, an internal error resulted in the wrong function being called, leading to the hack. This incident serves as a reminder of the importance of thoroughly checking and testing the security of the tools and processes we use and the potential consequences of human error.

2.4.6 Nomad Bridge Hacked

On August 2nd, the Nomad bridge, a cross-chain interoperability protocol, was attacked by hackers. The attack was made possible due to the fact that the trusted root of the Nomad Bridge Replica contract was incorrectly set to 0x0 during initialization, and the old root was not invalidated when the trusted root was modified. This allowed the attacker to construct arbitrary messages and steal funds from the bridge, resulting in a loss of more than $190 million. So far, more than 40 addresses have returned over $36 million to Nomad. This incident serves as a reminder of the importance of properly setting and updating security measures to prevent unauthorized access to our systems.

2.4.7 Elrond Suffers Security Breach

On June 5th, there was a suspected security breach on the Elrond blockchain network in which hackers "obtained" nearly 1.65 million $EGLD and sold it through the decentralized exchange Maiar. However, on June 8th, Elrond founder and CEO Beniamin Mincu tweeted that the issue had been resolved, all funds and users were safe, and almost all of the stolen funds had been recovered.

2.4.8 Mango Extracts $100 Million for Price Fixing

On October 12th, Mango, a Solana-based decentralized financial platform, tweeted about an incident in which hackers were able to extract funds from the platform through price manipulation of oracle machines. The attack occurred on the morning of October 1st, when two accounts funded by USDC held excessive positions in MNGO-ERP, causing the bottom price of MNGO/USD on various exchanges (such as FTX and Ascendex) to spike by 5-10% within a few minutes. This led to Switchboard and the Pyth oracle updating the MNGO benchmark price above $0.15, resulting in unrealized profits that increased the value of accounts holding MNGO-ERP to the point where they were able to borrow and withdraw large amounts of BTC (sollet), USDT, SOL, mSOL, and USDC. The total loan amount on the platform reached the equivalent of $190 million, with the net value withdrawn from the accounts being around $100 million. Mango is currently investigating the incident.

2.4.9 Harmony Loses Over $100 Million

On June 24th, the Harmony Horizon bridge was hacked, resulting in the attacker making more than $100 million in profit, including 11 ERC20 tokens, 13,100 ETH, 5,000 BNB, and 640,000 BUSD. According to the analysis by SlowMist MistTrack, the hack was not due to a smart contract vulnerability, but rather the leakage of a private key. Despite Harmony storing the private keys encrypted, the attacker was able to decrypt some of them and sign unauthorized transactions. Harmony's founder, Stephen Tse, addressed the incident on Twitter on June 26th and confirmed these details.

2.4.10 Qubit Losses $80 Million in Attack

The decentralized lending project QBridge, which operates on the BSC ecosystem, suffered a hack on its lending product Qubit. The hacker was able to mint a large amount of xETH collateral and consume around $80 million in assets from the fund pool. According to the analysis by SlowMist, the root cause of the attack was the failure to properly check for 0 addresses when transferring whitelisted tokens separately for ordinary tokens and native tokens. This allowed the hacker to exploit the recharge logic for ordinary tokens instead of going through the intended native recharge function. This incident serves as a reminder of the importance of implementing proper security checks and controls to prevent unauthorized access to our systems.

III. AML Analysis of Some Security Incidents

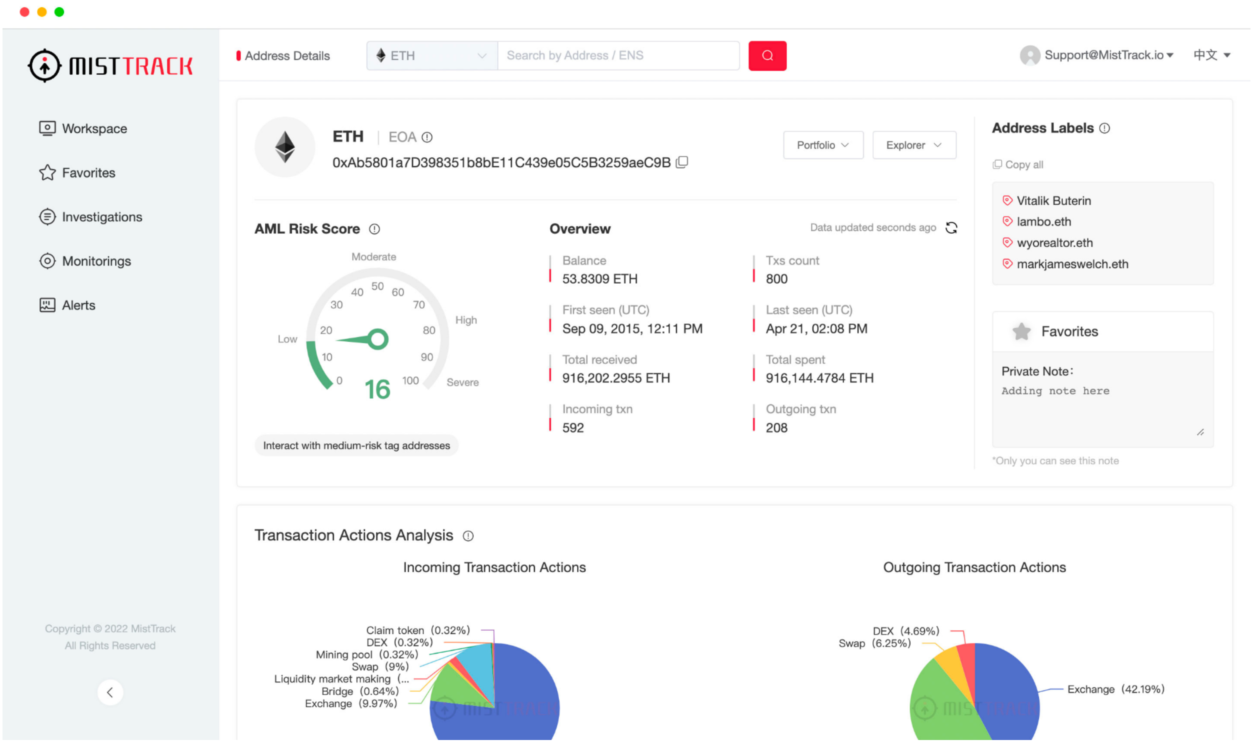
In our analysis of the intersection of anti-money laundering and security incidents, we will focus on the following key topics:

- Proposing a method for analyzing funds transferred out of currency mixers (such as Tornado.Cash and ChipMixer)
- Applying this anti-money laundering analysis method to analyze specific security incidents

3.1 Tools & Methods

Before we can begin our anti-money laundering analysis, it's important that we have the proper tools and methods in place to effectively handle complex cases of money laundering. This will ensure that our analysis is efficient and thorough.

3.1.1 Basic Tools - MistTrack



ETH | EOA
0xAb5801a7D398351b8bE11C439e05C5B3259aeC9B

AML Risk Score
16
Interact with medium-risk tag addresses

Overview
Data updated seconds ago

Balance
53.8309 ETH

Txs count
800

First seen (UTC)
Sep 09, 2015, 12:11 PM

Last seen (UTC)
Apr 21, 02:08 PM

Total received
916,202.2955 ETH

Total spent
916,144.4784 ETH

Incoming txn
592

Outgoing txn
208

Address Labels
Vitalik Buterin
lambo.eth
wyorealtor.eth
markjameswelch.eth

Favorites
Private Note:
Adding note here
*Only you can see this note

Transaction Actions Analysis
Incoming Transaction Actions
Outgoing Transaction Actions

(MistTrack Anti-Money Laundering Tracking System Example Diagram)

The MistTrack Anti-Money Laundering Tracking System is a software as a service (SaaS) system developed by SlowMist Technology that is designed to combat money laundering activities involving cryptocurrencies. It offers a range of core functions, including a fund risk scoring module, a transaction behavior analysis module, a fund traceability tracking module, and a fund monitoring module. These features allow for effective tracking and analysis of potentially illicit financial activities in the cryptocurrency space.

- **AML Risk Score**

The MistTrack anti-money laundering tracking system calculates the AML risk score for a given address by considering three factors: the entity that the address belongs to, the historical transaction activity of the address, and its interactions with the addresses in the SlowMist malicious address database. If the address belongs to a high-risk entity (such as a mixed currency platform) or has a history of capital transactions with known risk entities, it will be marked as a risky address. Additionally, addresses involved in verified illegal activities such as extortion, coin theft, and phishing scams will also be marked as risky based on the data in the SlowMist malicious wallet address database.

- **Address Labels**

The MistTrack anti-money laundering tracking system has collected and labeled over 200 million wallet addresses, which are grouped into 3 main categories:

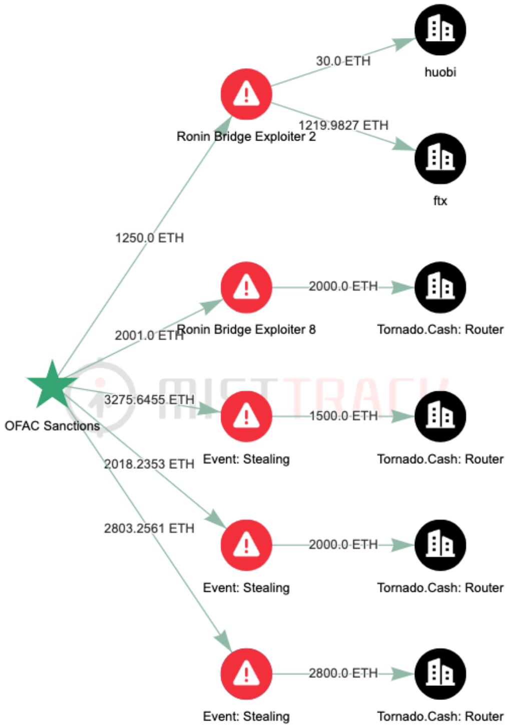
(1) The entity that the address belongs to (such as Coinbase or Binance)

(2) Its on-chain behavioral characteristics (such as being a DeFi Whale, MEV Bot, or ENS)

(3) Some off-chain intelligence data (such as having used imToken/MetaMask wallets)

- **Investigations**

The MistTrack anti-money laundering tracking system is designed to track and identify the flow of crypto assets across multiple blockchains, monitor fund transfers in real time, and provide a comprehensive view of both on-chain and off-chain information. It also offers strong technical support for the collection of judicial evidence. By utilizing these capabilities, we can more effectively identify and prevent illicit financial activities involving cryptocurrencies.



(MistTrack Tracking Analytics Example Map)

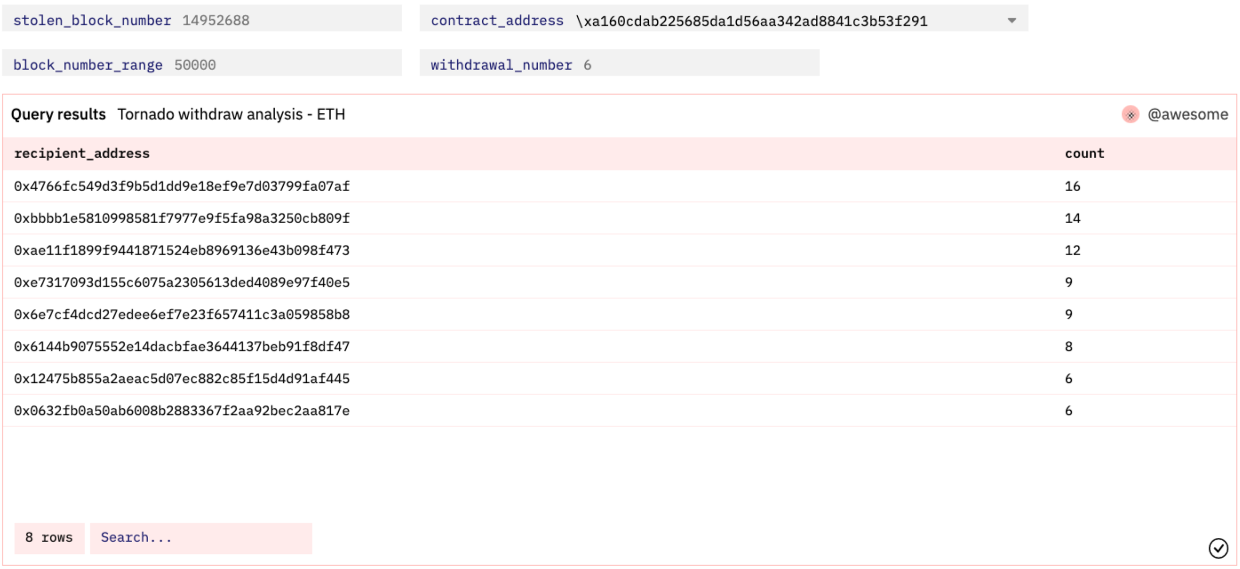
MistTrack is an essential tool for anti-money laundering analysis and research, providing comprehensive intelligence data assistance through the identification of over 1,000 entity addresses, 200+ million address labels, 100,000+ threat intelligence addresses, and over 90 million addresses associated with malicious activity. Its capabilities include transaction feature analysis, behavior portraits, and tracking investigations of any wallet address, all of which contribute to more effective and accurate anti-money laundering analysis and evaluation

3.1.2 Expanded Methodology - Data Analysis

While MistTrack is effective for common anti-money laundering analysis scenarios, it may be necessary to utilize additional methods in cases involving more complex or specialized situations. An example of this can be seen in the blockchain anti-money laundering fund landscape, where after several hack events, funds on the ETH/BSC chain have frequently been traced to a gray area - Tornado.Cash. This has made Tornado.Cash a key focus of anti-money laundering efforts on the ETH/BSC chain.

As new money laundering techniques emerge, it becomes necessary to develop new analysis methods to address them. One such method that is increasingly in demand is an analysis of transfers out of Tornado.Cash. Here is a proposed process for conducting this analysis:

- Record the available information, including the total amount transferred to Tornado.Cash, the time of the first Tornado.Cash deposit, and the block height of the first Tornado.Cash deposit.
- Input these parameters into the analysis panel.
- Obtain preliminary results for Tornado.Cash withdrawal data, then use feature classification to further filter the data.
- The resulting set of suspected hacker transfers is taken and verified, with the result set having the highest probability being the final conclusion for the Tornado.Cash transfer-out analysis.



stolen_block_number 14952688
contract_address \xa160cdab225685da1d56aa342ad8841c3b53f291
block_number_range 50000
withdrawal_number 6

Query results Tornado withdraw analysis - ETH

recipient_address	count
0x4766fc549d3f9b5d1dd9e18ef9e7d03799fa07af	16
0xbbbb1e5810998581f7977e9f5fa98a3250cb809f	14
0xae11f1899f9441871524eb8969136e43b098f473	12
0xe7317093d155c6075a2305613ded4089e97f40e5	9
0x6e7cf4dcd27edee6ef7e23f657411c3a059858b8	9
0x6144b9075552e14dacbfae3644137beb91f8df47	8
0x12475b855a2aeac5d07ec882c85f15d4d91af445	6
0x0632fb0a50ab6008b2883367f2aa92bec2aa817e	6

(Dune Dashboard - Tornado.Cash Transfer Out Analysis)

We have successfully applied this analysis method for Tornado.Cash fund transfers to several security incidents, including the Ronin Network hack, and was able to uncover the details of funds transferred from Tornado.Cash in each case.

It should be noted that this method of analyzing funds transferred out of Tornado.Cash has its limitations:

An additional limitation to consider when analyzing funds transferred out of Tornado.Cash is that the classification of these amounts is anonymous. As the amount of transferred funds increases, the number of corresponding anonymous sets decreases, and vice versa for smaller amounts. This means that it can be more challenging to analyze small amounts of funds.

On the BTC chain, it is common for hackers to use money laundering platforms such as ChipMixer and Blender, as seen in the blockchain anti-money laundering fund situation. Blender is currently sanctioned by the U.S. Department of the Treasury and is no longer available, so it will not be discussed further in this context.

Given the significant amount of money laundering activity that flows through ChipMixer, it is necessary to propose a method for analyzing ChipMixer fund transfers.

- Identify Withdrawal Features of ChipMixer

Input Address Type	Output Address Type	Input Amount Characteristics	Version	Lock Time
bech32(bc1q...)	bech32(bc1q...)	All input amounts meet the requirements of Chips (ie 0.001 * 2 to the nth power, n < 14)	2	Block Height - 1/ Block Height - 2/ Block Height - 3

- To analyze ChipMixer fund transfers, we can scan and screen the structured block data for the relevant time period based on the withdrawal characteristics described above, in order to identify ChipMixer withdrawal records within that time frame.

- Once the withdrawal record data has been obtained, it can be classified into various result sets. The result set with the highest probability can then be selected and verified.
- ChipMixer presents the conclusions of the analysis.

3.2 Detailed AML Analysis

3.2.1 Ronin Network

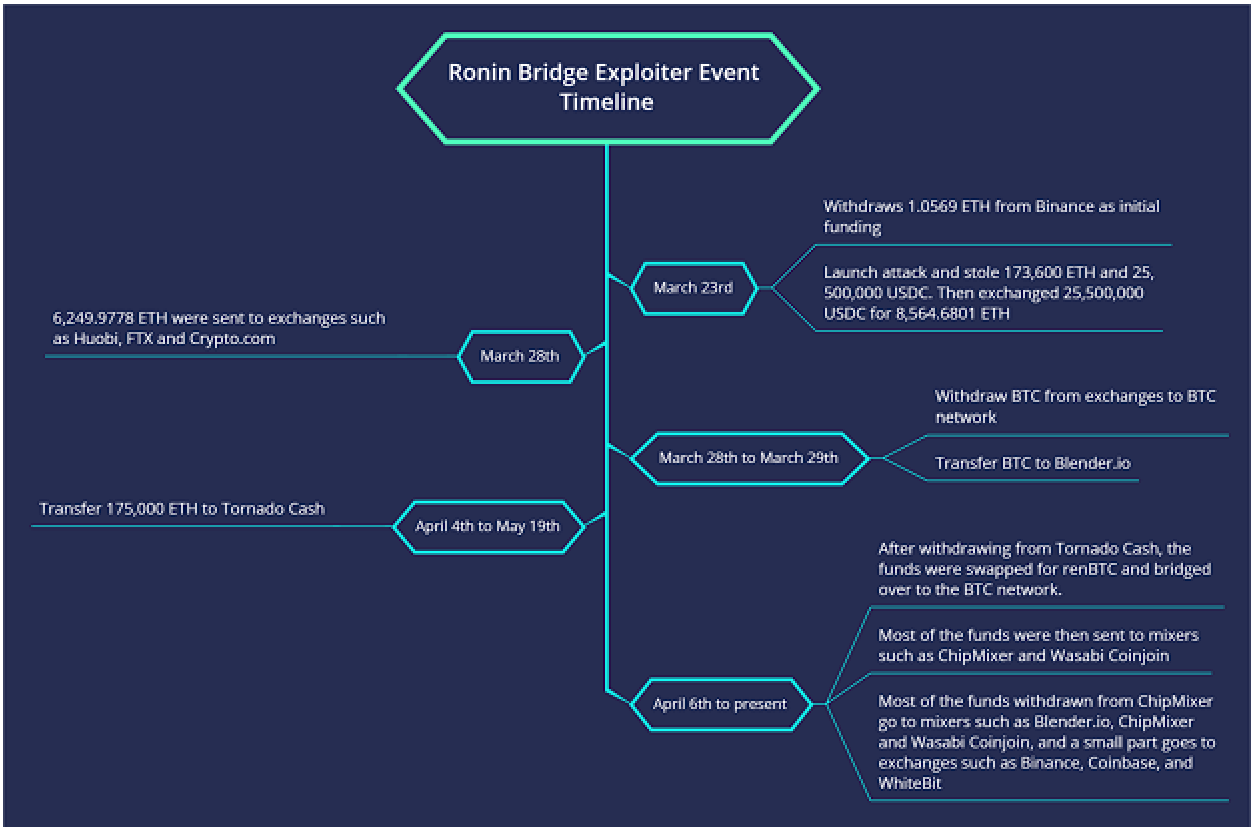
Hacker Address: 0x098B716B8Aaf21512996dC57EB0615e2383E2f96（ETH）

Date: March 23rd, 2022

Amount loss: 173,600 ETH、25,500,000 USDC

Initial funding: SimpleSwap

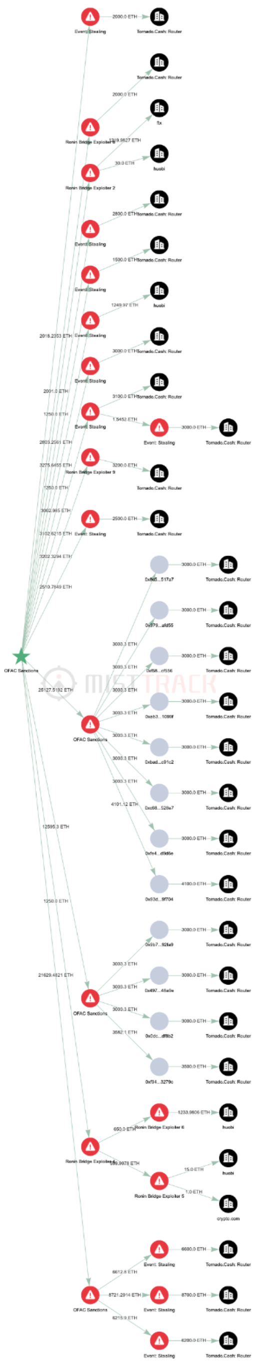
Event timeline:


Ronin Bridge Exploiter Event Timeline
March 23rd
Withdraws 1.0569 ETH from Binance as initial funding
Launch attack and stole 173,600 ETH and 25, 500,000 USDC. Then exchanged 25,500,000 USDC for 8,564.6801 ETH
March 28th
6,249.9778 ETH were sent to exchanges such as Huobi, FTX and Crypto.com
March 28th to March 29th
Withdraw BTC from exchanges to BTC network
Transfer BTC to Blender.io
April 4th to May 19th
Transfer 175,000 ETH to Tornado Cash
April 6th to present
After withdrawing from Tornado Cash, the funds were swapped for renBTC and bridged over to the BTC network.
Most of the funds were then sent to mixers such as ChipMixer and Wasabi Coinjoin
Most of the funds withdrawn from ChipMixer go to mixers such as Blender.io, ChipMixer and Wasabi Coinjoin, and a small part goes to exchanges such as Binance, Coinbase, and WhiteBit

(Ronin Bridge Exploiter Timeline of Fund Transfers)

ETH Fund Transfers

The hacker was able to exchange the 25.5 million USDC gained from the attack for 8,562.6801 ETH, bringing the total amount of ETH that needed to be laundered to 182,163.737 (1.0569 ETH withdrawn from Binance, 173,600 ETH obtained from the attack, and 8,562.6801 ETH obtained from converting USDC from the attack).



(Ronin Bridge Exploiter Map of Fund Transfers)

The following is a breakdown of the hacker's profit flow to various entities:

Entity	Funds Transferred
Tornado.Cash	175,100 ETH
Huobi	5,028.9951 ETH
FTX	1,219.9827 ETH
Crypto.com	1 ETH
Balance	667.3916 ETH

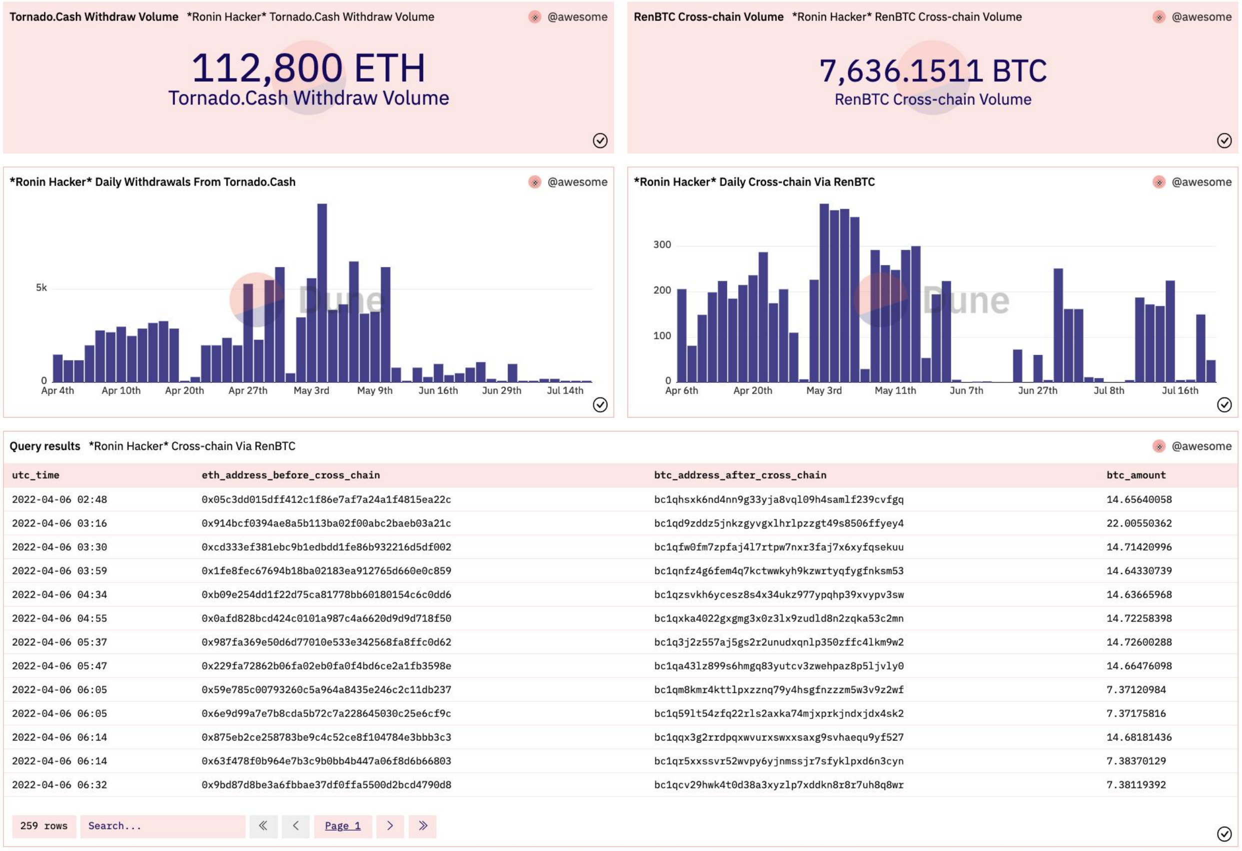
Note: The other flowing funds that are not included in this table are losses incurred during the money laundering process.

Tornado.Cash Fund Transfers

The Ronin hacker transferred a total of 175,100 ETH to Tornado.Cash. Upon analysis, we determined that the hacker's withdrawal from Tornado.Cash exhibited the following characteristics:

Use of 1inch or Uniswap to convert to renBTC and then cross-chain to the BTC chain through renBTC after transferring out from Tornado.Cash or after transferring a layer

Using Dune Analytics, we screened for Tornado.Cash withdrawals and cross-chain to BTC chain data that met the above characteristics and effectively visualized the results, as shown in the figure below:



Tornado.Cash Withdraw Volume *Ronin Hacker* Tornado.Cash Withdraw Volume

112,800 ETH
Tornado.Cash Withdraw Volume

RenBTC Cross-chain Volume *Ronin Hacker* RenBTC Cross-chain Volume

7,636.1511 BTC
RenBTC Cross-chain Volume

Ronin Hacker Daily Withdrawals From Tornado.Cash

Ronin Hacker Daily Cross-chain Via RenBTC

Query results *Ronin Hacker* Cross-chain Via RenBTC

utc_time	eth_address_before_cross_chain	btc_address_after_cross_chain	btc_amount
2022-04-06 02:48	0x05c3dd015dff412c1f86e7af7a24a1f4815ea22c	bc1qhsxk6nd4nn9g33yja8vql09h4samlf239cvfgq	14.65640058
2022-04-06 03:16	0x914bcf0394ae8a5b113ba02f00abc2baeb03a21c	bc1qd9zddz5jnkzgyvgxlhrlpzzgt49s8506ffyey4	22.00550362
2022-04-06 03:30	0xcd333ef381ebc9b1edbdd1fe86b932216d5df002	bc1qfw0fm7zpfaj4l7rtpw7nxr3faj7x6xyfqsekuu	14.71420996
2022-04-06 03:59	0x1fe8fec67694b18ba02183ea912765d660e0c859	bc1qnfz4g6fem4q7kctwwkyh9kzwrtyqfygfnksm53	14.64330739
2022-04-06 04:34	0xb09e254dd1f22d75ca81778bb60180154c6c0dd6	bc1qzsvkh6ycesz8s4x34ukz977ypqhp39xvypv3sw	14.63665968
2022-04-06 04:55	0x0afd828bcd424c0101a987c4a6620d9d9d718f50	bc1qxka4022gxgmg3x0z3lx9zudld8n2zqka53c2mn	14.72258398
2022-04-06 05:37	0x987fa369e50d6d77010e533e342568fa8ffc0d62	bc1q3j2z557aj5gs2r2unudxqnlp350zffc4lkm9w2	14.72600288
2022-04-06 05:47	0x229fa72862b06fa02eb0fa0f4bd6ce2a1fb3598e	bc1qa43lz899s6hmgq83yutcv3zwehpaz8p5ljvly0	14.66476098
2022-04-06 06:05	0x59e785c00793260c5a964a8435e246c2c11db237	bc1qm8kmr4kttlpxzznq79y4hsgfnzzzm5w3v9z2wf	7.37120984
2022-04-06 06:05	0x6e9d99a7e7b8cda5b72c7a228645030c25e6cf9c	bc1q59lt54zfq22rls2axka74mjxprkjndxjdx4sk2	7.37175816
2022-04-06 06:14	0x875eb2ce258783be9c4c52ce8f104784e3bbb3c3	bc1qqx3g2rrdpqxwvurxswxxsaxg9svhaequ9yf527	14.68181436
2022-04-06 06:14	0x63f478f0b964e7b3c9b0bb4b447a06f8d6b66803	bc1qr5xxssvr52wvpy6yjnmssjr7sfyklpxd6n3cyn	7.38370129
2022-04-06 06:32	0x9bd87d8be3a6fbbae37df0ffa5500d2bcd4790d8	bc1qcv29hwk4t0d38a3xyzlp7xddkn8r8r7uh8q8wr	7.38119392

(Ronin Hackers Transfer Data Across Chains via renBTC after Transfer from Tornado.Cash)

The analysis chart above led to the creation of the following table, which shows the funds transferred out of Tornado.Cash:

Transfer Method	Funds Transferred
Amount of renBTC bridged BTC Blockchain	112,800 ETH
Balance in Tornado.Cash	62,300 ETH

Note: The data is valid as of July 20th.

BTC Fund Transfers

Based on our analysis of Tornado.Cash fund transfers, we determined that a total of 8,075.9329 BTC were transferred across chains to the BTC chain with characteristics that match those of the Ronin hacker. Of these, 6,191.2542 BTC were confirmed to be related to the hacker, while an additional 439.7818 BTC were withdrawn from Huobi and FTX. This brings the total amount of confirmed funds belonging to the Ronin hacker to 6,631.036 BTC. The following table shows the further transfer of these funds.

Entity	Funds Transferred
ChipMixer	3460.6845 BTC
Blender	439.7818 BTC
Wasabi Coinjoin	55.1448 BTC
renBTC	95.6871 BTC
Coinbase	0.5632 BTC
ChangeHero	0.488 BTC
Binance	12.0973 BTC
Wirex	0.0399 BTC
Kuna	0.0384 BTC
Any.Cash	0.0676 BTC
Unknown	153.0143 BTC
Balance	2413.4292 BTC
Total	6631.036 BTC

Note: Transfers below 0.1 BTC are not considered.

ChipMixer Fund Transfers

Based on the BTC fund transfer data, we see that 3460.6845 BTC was transferred to ChipMixer. By analyzing the withdrawal data from ChipMixer and monitoring the BTC chain, we were able to identify that the Ronin hackers withdrew a total of 2,871.03 BTC from ChipMixer. The following table shows the further transfer of these funds.

Entity	Funds Transferred
Blender	1356.0 BTC
Wasabi Coinjoin	9.8365 BTC
ChipMixer	547.7938 BTC
UnKnown	681.4247 BTC
Balance	235.4739 BTC

Note: Transfers below 0.1 BTC are not considered.

3.2.2 Wormhole

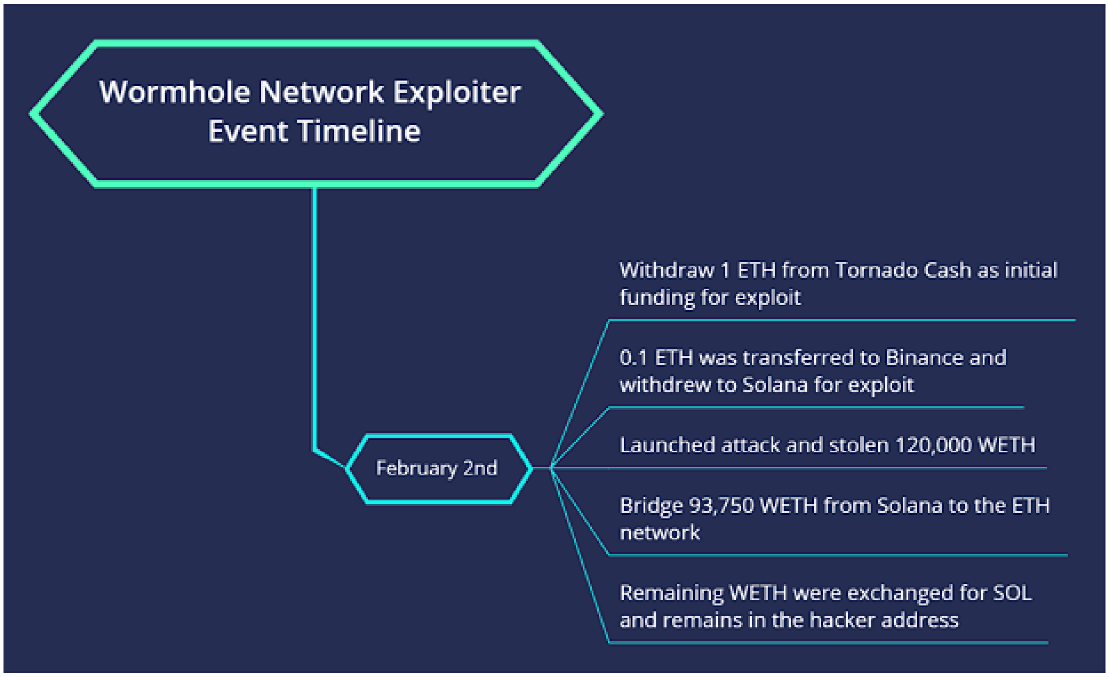
Hacker Address: CxegPrfn2ge5dNiQberUrQJkHCcimeR4VXkeawcFBBka (Solana)

Date: February 2nd, 2022

Amount loss: 120,000 WETH

Initial funding: Tornado.Cash

Event timeline:



Wormhole Network Exploiter Event Timeline

February 2nd

Withdraw 1 ETH from Tornado Cash as initial funding for exploit

0.1 ETH was transferred to Binance and withdrew to Solana for exploit

Launched attack and stolen 120,000 WETH

Bridge 93,750 WETH from Solana to the ETH network

Remaining WETH were exchanged for SOL and remains in the hacker address

(Wormhole Network Exploiter Timeline of Fund Transfers)

WETH Fund Transfers

Transfer Method	Funds Transferred
Bridge to ETH Blockchain	93,750 WETH
Converted to SOL	26,250 WETH

Hacker Address Balance

Address	Balance
CxegPrfn2ge5dNiQberUrQJkHCcimeR4VXkeawcFBBka	432,661.15 SOL
0x629e7da20197a5429d30da36e77d06cdf796b71a	93,750.623 ETH

3.2.3 Beanstalk Farms

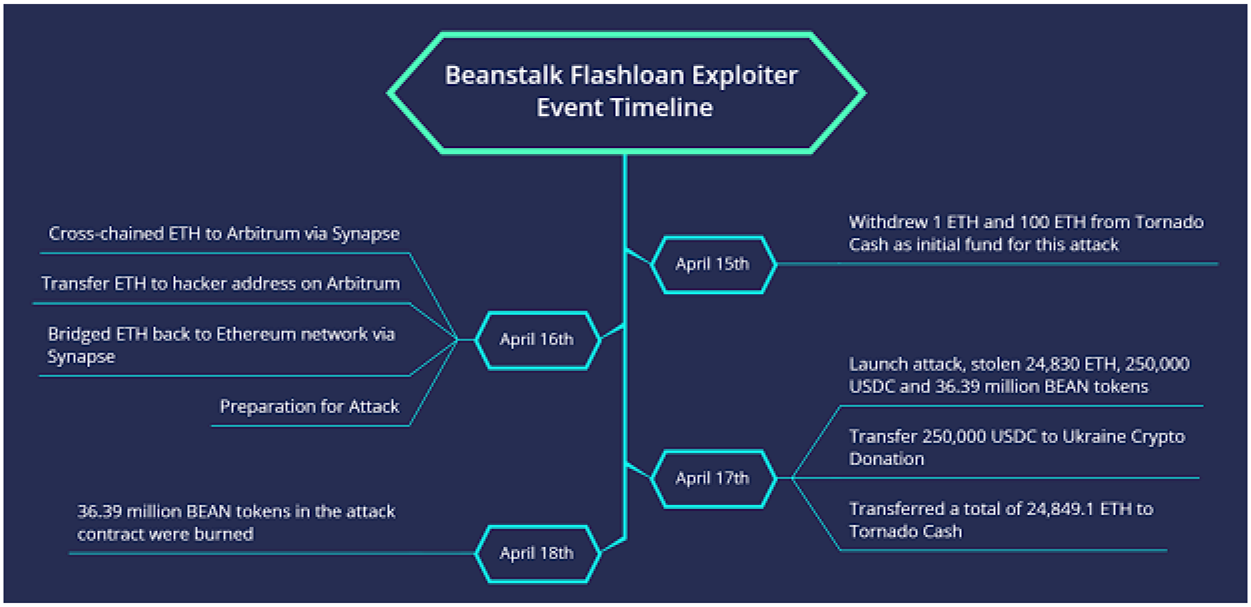
Hacker Address: 0x1c5dCdd006EA78a7E4783f9e6021C32935a10fb4(ETH)

Date: April 17th, 2022

Amount loss: 24,830 ETH、250,000 USDC Tokens & 36,390,000 BEAN Tokens

Initial funding: Tornado.Cash

Event timeline:



Beanstalk Flashloan Exploiter Event Timeline

April 15th

Withdrew 1 ETH and 100 ETH from Tornado Cash as initial fund for this attack

April 16th

Cross-chained ETH to Arbitrum via Synapse

Transfer ETH to hacker address on Arbitrum

Bridged ETH back to Ethereum network via Synapse

Preparation for Attack

April 17th

Launch attack, stolen 24,830 ETH, 250,000 USDC and 36.39 million BEAN tokens

Transfer 250,000 USDC to Ukraine Crypto Donation

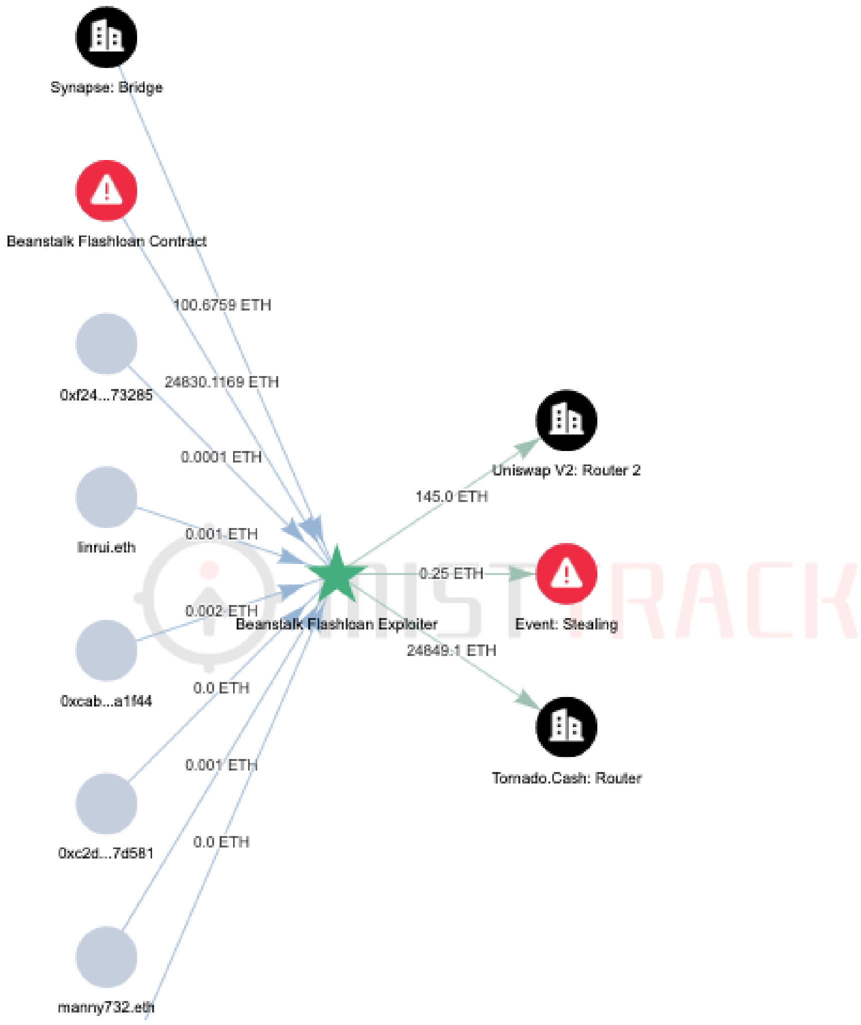
Transferred a total of 24,849.1 ETH to Tornado Cash

April 18th

36.39 million BEAN tokens in the attack contract were burned

(Beanstalk Flashloan Exploiter Timeline of Fund Transfers)

ETH Fund Transfers



(Beanstalk Flashloan Exploiter Map of ETH Fund Transfers)

The following table displays the transfer of funds from ETH:

Entity	Funds Transferred
Tornado.Cash	24849.1 ETH

Note: The transferred funds include the remaining funds from the attack fee.

3.2.4 Harmony

Hacker Address:

0x0d043128146654C7683Fbf30ac98D7B2285DeD00(ETH)

0x0d043128146654C7683Fbf30ac98D7B2285DeD00(BSC)

Date: June 23rd

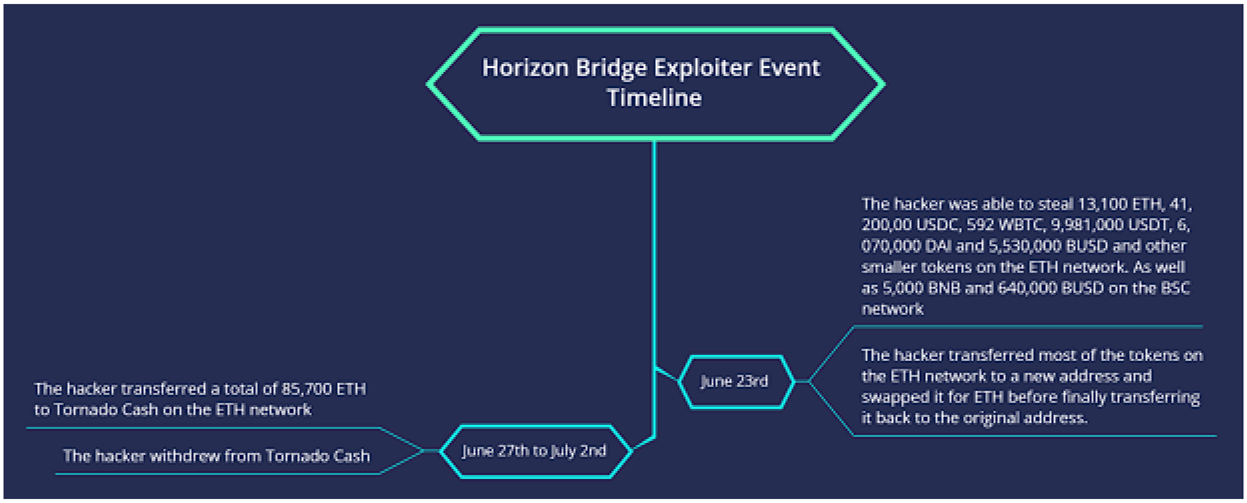
Amount Loss:

ETH: 13,100 ETH, 41,200,000 USDC, 592 WBTC, 9,981,000 USDT, 6,070,000 DAI, 5,530,000 BUSD, 84,620,000 AAG, 110,000 FXS, 415,000 SUSHI, 990 AAVE, 43 WETH, & 5,620,000 FRAX

BSC: 5,000 BNB & 640,000 BUSD

Initial Funding: N/A

Event Timeline:



Horizon Bridge Exploiter Event Timeline

June 23rd

The hacker was able to steal 13,100 ETH, 41, 200,00 USDC, 592 WBTC, 9,981,000 USDT, 6, 070,000 DAI and 5,530,000 BUSD and other smaller tokens on the ETH network. As well as 5,000 BNB and 640,000 BUSD on the BSC network

The hacker transferred most of the tokens on the ETH network to a new address and swapped it for ETH before finally transferring it back to the original address.

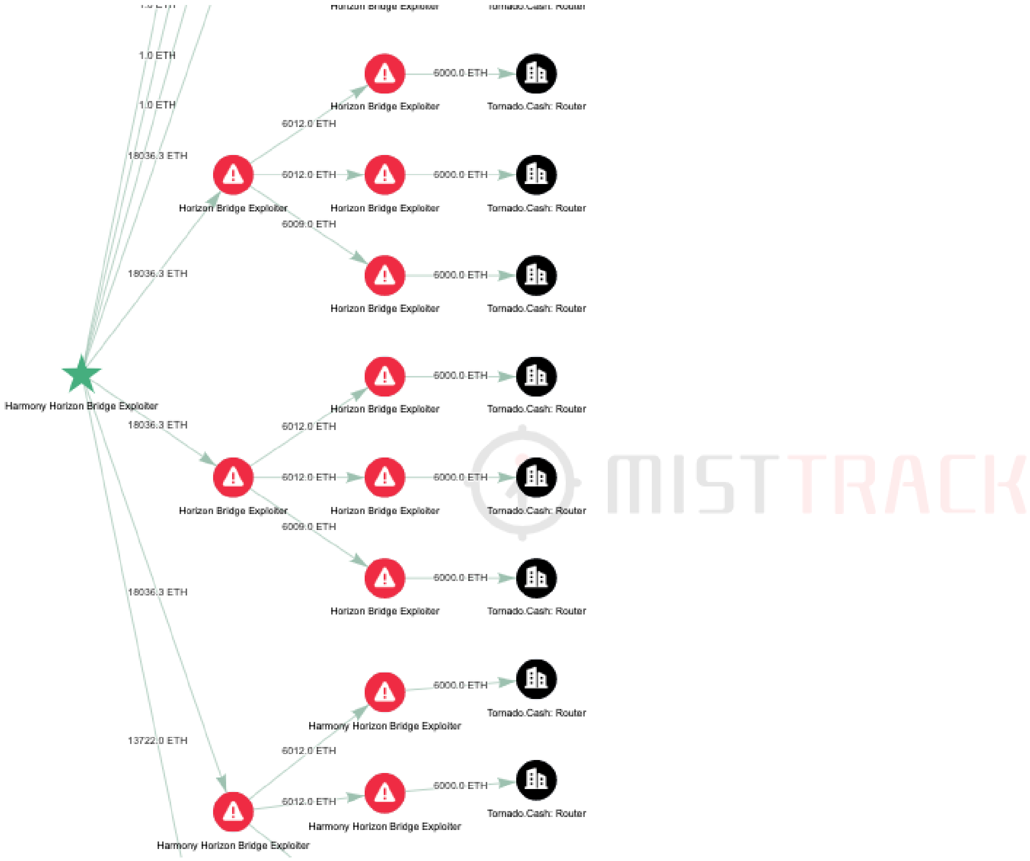
June 27th to July 2nd

The hacker transferred a total of 85,700 ETH to Tornado Cash on the ETH network

The hacker withdrew from Tornado Cash

(Horizon Bridge Exploiter Timeline of Fund Transfers)

ETH Fund Transfers



(Horizon Bridge Exploiter Map of ETH Fund Transfers)

ETH Transfer Chart:

Entity	Funds Transferred
Tornado.Cash	85,700 ETH
Balance	201.2094 ETH

Tornado.Cash Transfer

The hackers sent a total of 85,700 ETH to Tornado Cash. After our analysis, we concluded that the following withdrawals met the criteria for the Harmony hacker:

- Tornado Cash withdrawals were performed in batches. The number of withdrawals per address was fixed. Each address received 5 to 6 withdrawals, implying that either 5 * 100 ETH or 6 * 100 ETH was sent to the withdrawal address.

- Following the completion of the withdrawal from Tornado Cash, the funds remained relatively unmoved for close to a month.

According to the Tornado Cash withdrawal characteristics provided above, a total of 83,300 ETH withdrawals had ties to the hackers.

ETH Transfer Chart：

Entity	Funds Moved
Tornado Cash	83,300 ETH

IV. Outlook

What are some other things we should be keeping an eye on in the cryptocurrency world in 2023?

1. Regulatory Compliance

Regulatory issues have become a major concern in the cryptocurrency world, especially after events like the FTX thunderstorm. Cryptocurrency projects operate like banks, but they don't have the same rules and regulations that banks do. One of the most pressing problems at the moment is figuring out how to effectively supervise this market so that consumers are protected and can be compensated if the project experiences losses, and how to make the market more stable. On the positive side, it's a good sign that regulators and the general public are gaining a better understanding of cryptocurrency and blockchain technology, and that countries are starting to clarify their policies and attitudes towards cryptocurrency. This will allow the market to continue growing in a more regulated and compliant manner.

2. Increased Focus on Security Audits

In 2022, there were numerous security incidents, particularly between October 1st and October 15th, when nearly 20 Web3 projects and trading platforms were attacked. These attacks were often the result of security vulnerabilities in the project code. This highlights the fact that while the blockchain ecosystem is thriving and growing, code security should bel a top priority for projects.

For example, many cross-chain bridges have been rushed to market in order to quickly attract users and project parties with zero fees, but they often neglect the most important aspect of security - multi-signature wallets. If a hacker can control the signature, they can control everything. Additionally, cross-chain bridges often skip security audits from agencies and are rarely monitored by the community, making them prime targets for hackers. As more and more security incidents occur, it's likely that projects will realize the importance of security audits. At SlowMist, we have a strong background in blockchain security and always recommend teams to conduct comprehensive front-end and contract security audits before going live. Additionally, releasing a Bug Bounty can help prevent security issues and improve the overall security level of the project during its ongoing operation and development.

3. Continued Expansion where Multiple Chains Coexist Harmoniously

In 2021, major public chains like Solana and Avalanche will gain significant attention from investors. In 2022, emerging public chains like Aptos and Sui will also receive high levels of investment and attention. Although Ethereum has switched to a more energy-efficient proof-of-stake mechanism (PoS) after the merger, there has been no change in terms of fees and transaction speed, and the competition to expand will continue to heat up. Other public chains are looking to increase their throughput through different methods, reduce transaction costs, and attract top developers in order to compete for market share. In recent years, Ethereum projects have been built on scalable Layer 2 platforms like Rollup and Arbitrum in order to reduce the burden on the Layer 1 network, improve business processing efficiency, and achieve expansion. These platforms will continue to be seen as a mid-to long-term solution to Ethereum's network congestion problem. At the same time, the future will likely see the coexistence of multiple chains as it is difficult for one blockchain to meet the needs of all users. To that end, it is important to solve interoperability and compatibility issues between chains and make sure that EVM-compatible and non-EVM chains are well-connected. The interoperability impossible triangle problem should also be weakened and cross-chain bridges should have fast enough speeds and provide a smooth and safe user experience.

4. AML & On-chain Tracking Analytics

As the number of hacking incidents increases, the importance of tracking and analysis on the blockchain has become more evident. Currently, mainstream blockchain browsers mainly focus on querying information on-chain, but querying is only the most basic function of these browsers. In addition to querying, data on-chain can also be used for data recovery and anti-money laundering purposes. There are various on-chain tracking and analysis tools and platforms available that allow users to check if their assets are connected to dirty money and to find information such as the whereabouts of funds through data aggregation. In the future, tracking tools will likely continue to evolve and become even more powerful in the fight against money laundering.

5. Increased Focus on Backups

Backing up encrypted asset ownership, such as private keys or mnemonic phrases, is essential because they hold complete ownership of the cryptocurrency. If these backups are stolen or lost, all assets will be lost as well. This is a major weakness in the field of encrypted assets. There are many products available to ensure the safe use of assets in various scenarios, whether it's a hot wallet or a cold wallet, but it's easy to overlook the importance of backups. In most cases of stolen or lost coins, the problem lies with the leakage or loss of private key/mnemonic backups. Backups are just as important as the encrypted assets themselves and must be treated with the same level of importance. In recent months, a new technology called multi-party computation (MPC) has been getting a lot of attention as a way to solve the single-point backup problem. With MPC, the initial private key is split into multiple shards and distributed to a group of people. When recovery is needed, a specific program is used to restore the original private key. The use of MPC in combination with multi-signature technology shows great promise and should be promoted as soon as possible. It would be great if an open source solution that meets industry-recognized standards could be developed in the near future.

6. Zero-Knowledge Proof: Scaling & Privacy

Zero-knowledge proof is a method that allows the prover to convince the verifier that a certain conclusion is correct without revealing any useful information to the verifier. It's a branch of cryptography that has the potential to solve scaling and privacy issues for many Layer 1 blockchain projects. While it's not a new term, it's only recently become a hot topic and may be one of the most important solutions for Web3 and the blockchain in the coming years.

V. Summary

Throughout 2022, the word 'turmoil' has been a constant presence. Despite the ongoing aftermath of turbulence and the current 'crypto winter', the development of the blockchain industry cannot be stopped. By being cautious and working towards the betterment of the industry, we can ensure its long-term stability. Despite the challenges, we remain optimistic about the development of the blockchain industry in 2023.

VI. Disclaimer

This report is based on our understanding of the blockchain industry, as well as data from SlowMist Hacked and MistTrack, an anti-money laundering tracking system. However, due to the anonymous nature of the blockchain, we cannot guarantee the absolute accuracy of all the data and cannot be held responsible for any errors, omissions, or losses that may result from the use of this report. It should also be noted that this report is not intended to be used as investment advice or any other type of analysis.

If there are any omissions or deficiencies in this report, we welcome constructive criticism and corrections.

VII. 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), Staking and other SaaS products. We have partnerships with domestic and international firms such as Akamai, Cloudflare, 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

Safety Monitoring

Dynamic security monitoring for all possible vulnerabilities

Blockchain Threat Intelligence

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

Bug Bounty

Monetary reward to ethical hackers for discovering and reporting vulnerability

Defense Deployment

Systematic defense plan adapted to local conditions

Security Consulting

Guide the construction of pioneering safety system

Hacking Time

Annual close-door training focusing on blockchain security

Digital Asset Security Solution

Open source digital asset security solutions

Security Services

SlowMist AML

Block risky cryptocurrencies and avoid risk

MistTrack

A crypto tracking and compliance platform for everyone

Vulnerability Monitoring Vulpush

First-hand security vulnerability intelligence in real time

SlowMist Hack

Full Summary of blockchain attack events

False Top-up Vulnerability Scanner

Creating safe deposit and withdrawals for trading platform

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 Public Account

SLOWMIST

Focusing on Blockchain Ecosystem Security