2022 Mid-Year

Blockchain Security and AML Analysis Report

SLOWMIST

Table of contents

This report focuses on important events in the blockchain industry in the first half of 2022, primarily involving the security state of different blockchain platforms, extending and extracting typical security events and common attack techniques that happened in the first half of the year. This report also examines the flow of stolen money in these popular security incidents, and for the first time, it provides a summary that involves a sophisticated analytical approach of monitoring coin mixing funds.

1. Background

1.1 Supervision of Blockchain Ecosystem

The global social and economic development has faced unprecedented problems in the last two years as a result of numerous causes such as a pandemic, economic slump, energy constraint, escalation of geopolitical conflicts, and increased worldwide rivalry. At the same time, the global blockchain sector is experiencing rapid change: blockchain technology's efficiency, security, and scalability have continued to progress, as the advent of emergent areas such as the Metaverse and NFT marketplace has allowed blockchain to thrive. The industry has now entered the 3.0 age.

From the standpoint of policy oversight, as regulatory agencies and the general public get a better grasp of cryptocurrencies and blockchain technology, the regulations of various nations in the area of cryptocurrency are diverging dramatically. Governments throughout the globe have three approaches to cryptocurrency regulation: welcoming support, ambiguous restrictions, and rigorous limitations. Although governments' views toward cryptocurrencies vary, based on laws implemented in the first half of the year, 2022 will surely mark the start of a new age of crypto regulation, as the cryptocurrency industry is heading toward compliance.

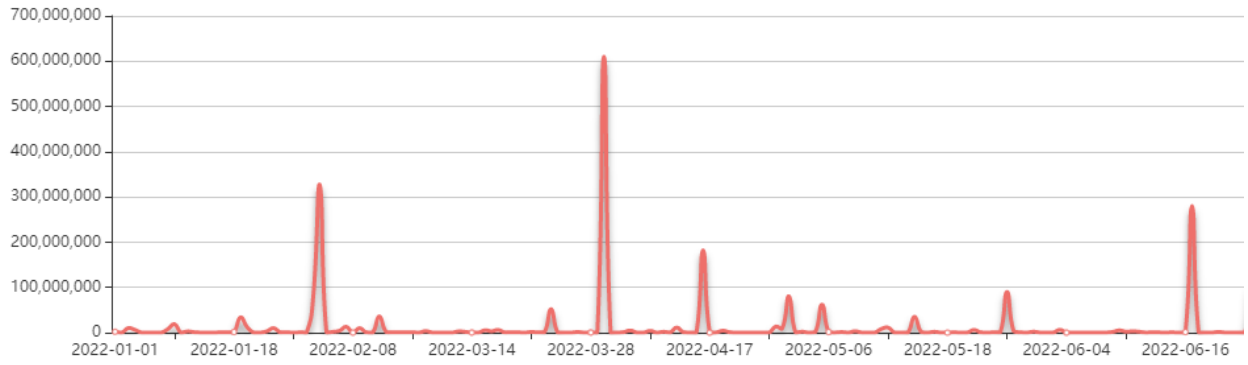
Opportunities and obstacles for the growth of the blockchain sector coexist from the standpoint of industrial empowerment. Blockchain technology is progressing from "accessible" to "user-friendly." Blockchain is accelerating the integration with traditional industries in the context of promoting the digital transformation of various industries, such as the explosive growth of blockchain "dual-carbon" applications, which not only represents the urgent global need to

address climate change and promote sustainable development, but also represents the rapid integration of the "green revolution" and emerging technologies. Furthermore, the rapid rise of smart contract applications, the emergence of new industry blockchains, and the arrival of additional applications in data and other industries, demonstrate that blockchain is playing an increasingly important role in driving business throughout a variety of fields.

In terms of market development, cryptocurrencies experienced incredible turmoil in the first half of the year due to the collapse of prices, the collapse of the DeFi protocols, and the bankruptcy of CeFi. On the other hand, many emerging trends and themes are forming, the number of cryptocurrency users and Web3 developers are increasing overall and the form of the meta-universe is gradually emerging. The cumulative international cryptocurrency market value as of June 30 topped $905.1 billion, according to CoinMarketCap statistics, and the global blockchain industry as a whole is still thriving.

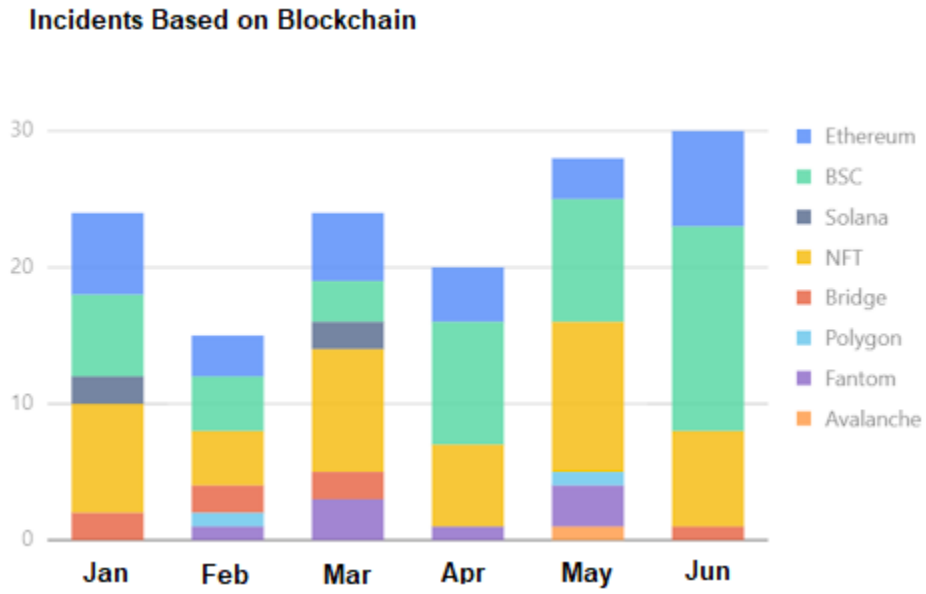
1.2 Blockchain Security

As the general growth trend of the blockchain industry improves, bitcoin fraud is also becoming more prevalent. According to the SlowMist Hacked, there were 187 security incidents in the first half of 2022, with damages totaling $1.976 billion as of June 30.



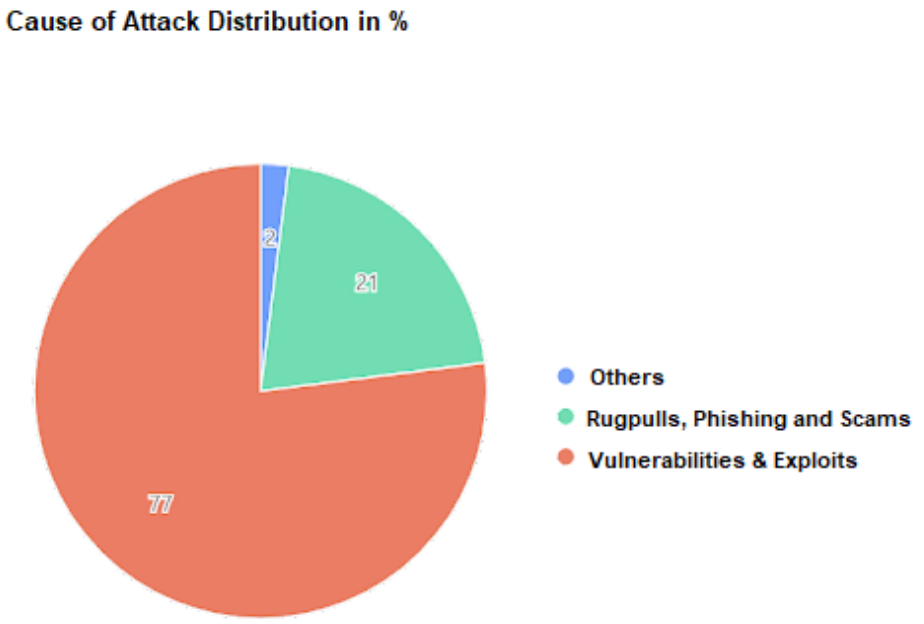
(2022 - Security Incidents in First Half of the Year)

According to statistics, the months with the highest number of safety incidents in the first half of the year were primarily May and June. From the perspective of individual ecosystems, a majority of security incidents occurred on the BSC and cross-chain bridges incurred the most losses.

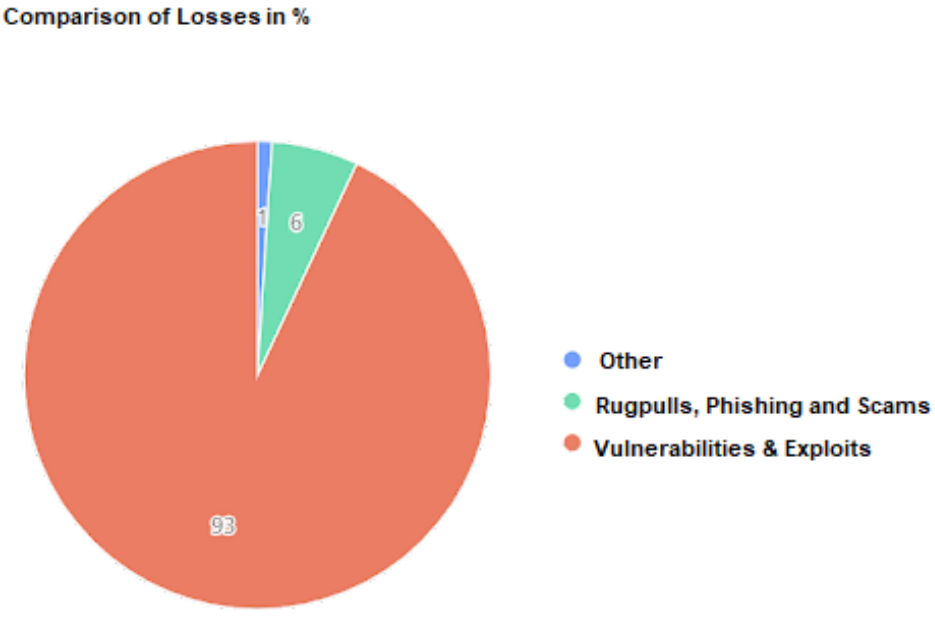


(2022 - Distribution of Events for Each Blockchain by Month in First Half of the Year)

Approximately 77% (144 cases) of these security incidents resulted from the project's own vulnerabilities being exploited by attackers, with a loss of approximately $1.84 billion, accounting for 93% of the total loss from security incidents. Approximately 21% (39 cases) resulted from Scams including Phishing & Rug Pull attacks, with a loss totalling approximately $130 million. This accounted for 7% of the total loss from security incidents.



(2022 - Cause of Attack Distribution in First Half of the Year)



(2022 - Comparison of Losses in First Half of the Year)

1.3 Blockchain Anti-Money Laundering Status

Cryptocurrency transactions are inherently anonymous and irrevocable. Because of this, in the case of common cryptocurrency scams, blockchain anti-money laundering is in a critical position and also serves as the final line of defense to prevent hackers from effectively exploiting it. In response to the omnipresent danger of hackers, many entities, including trading platforms/money management platforms/project contributors, regulators, and blockchain security businesses, have established anti-money laundering coalitions.

These organizations' anti-money laundering dynamics in the first half of 2022 are as follows:

Platform for trading/money management/project contributors

Tether: In the first half of 2022, 132 ETH addresses were blacklisted and the USDT-ERC20 assets held on these addresses were frozen.
Circle: In the first half of 2022, 18 ETH addresses were blacklisted and the USDC-ERC20 assets held on these addresses were frozen.

Regulations

On April 14, the US Treasury Department sanctioned Ronin Network hacker (LAZARUS GROUP) associated addresses, and on May 6, it sanctioned a bitcoin mixer, Blender. It is worth mentioning that the US Treasury Department has never before authorized a bitcoin mixer.

Blockchain Security Company

Chainalysis: On March 10th, an on-chain database contract called SanctionsList was formed, banning a total of 31 addresses.
SlowMist: On April 27th, the MistTrack anti-money laundering monitoring system, which focuses on preventing cryptocurrency money laundering operations, was formally introduced.

As we all know, the major force of money laundering has always been hackers, darknet organizations, fraudsters, and Rug Pull projects that have constructed blockchain security breaches. The most infamous of them is the North Korean hacking outfit LAZARUS GROUP, which presents a significant danger to the Blockchain ecosystem.

According to open source intelligence and on-chain data analysis, The Lazarus Group's dynamics in the first half of the year are as follows:

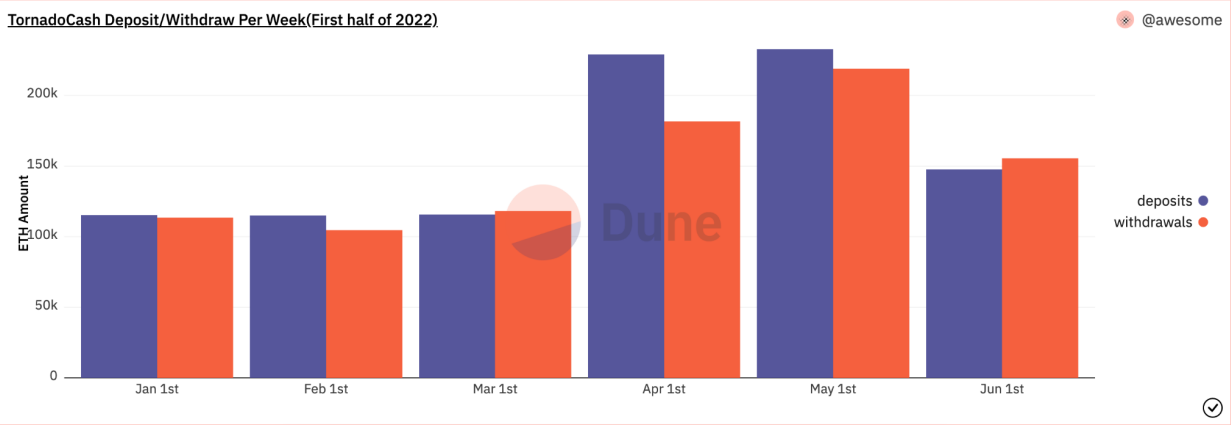
1. On January 17th, Crypto.com had unauthorized withdrawals made from a limited number of user accounts.
2. On February 8th, the IRA Financial Gemini escrow account was illegally withdrawn.
3. On March 23rd, the incident on the Ronin Network bridge became one of the most costly hacking events in crypto history.

We can find traces of the Lazarus Group in these security incidents through systematically monitoring their money laundering techniques.

- Initial stage: Convert all stolen funds on the ETH network to ETH and transfer all ETH to Tornado Cash (in large quantities) or a trading platform (small amount).
- Middle stage: Funds withdrawn from Tornado Cash were in batches and converted into renBTC tokens before being transferred over to the BTC blockchain.
- Later stage: After withdrawing renBTC, the funds were pooled and transferred to Coinjoin, a mixer on the bitcoin blockchain.

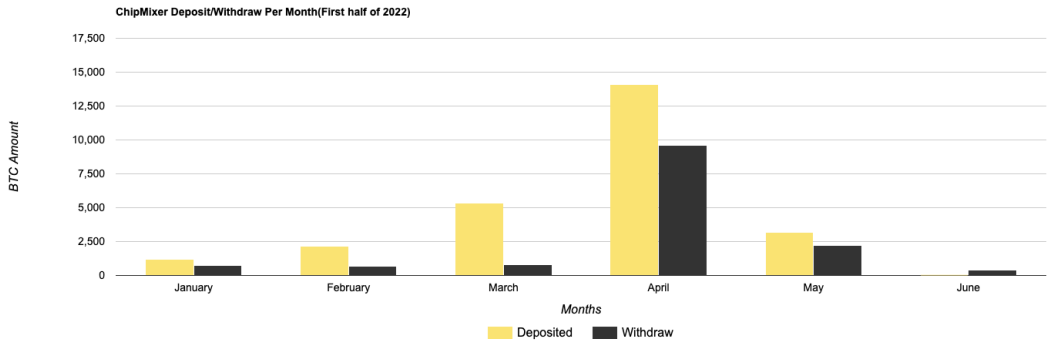
Money laundering tools are obviously necessary in the process of money laundering by hackers, darknet organizations, fraudsters, and Rug Pull scammers. Tornado Cash is a common money laundering platform on the ETH and BSC chain. Coinjoin tools (ChipMixer, for example), coin mixers (Blender, CryptoMixer, for example), private wallets (Wasabi, Samourai, for example), currency exchange platforms (ChangeNOW, SimpleSwap, FixedFloat, for example), and certain trading platforms are all accessible on the bitcoin blockchain.

The following are deposits and withdrawal figures for various typical money laundering incidents in the first half of 2022:



(Tornado Cash Deposit/Withdrawal Chart for the First Half of the Year)

Tornado Cash: Users deposited a total of 955,277 ETH ~$2.442 billion to Tornado Cash in the first half of 2022. A total of 892,573 ETH ~$2.249 billion was withdrawn from Tornado Cash.



(ChipMixer Deposit/Withdrawal Chart for First Half of the Year)

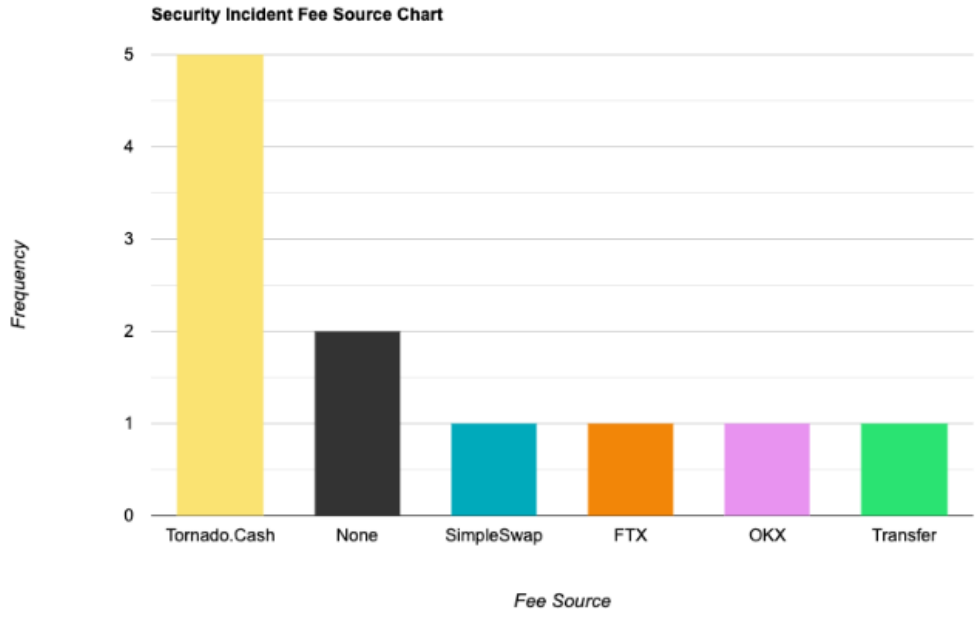
ChipMixer: In 2022, 26,021.89 BTC was sent to ChipMixer, and 14,370.57 BTC were withdrawn from ChipMixer.

Blender: This coin mixer was used by Lazarus Group to launder funds stolen from the Ronin Network's bridge. On May 6, the US Treasury Department sanctioned it, and now the website is no longer accessible.

Several key concerns arise throughout the anti-money laundering analysis process: where does the initial funding for the attack originate from? Where were the funds transferred to? We will now

investigate these two questions based on these security incidents that happened in the first half of 2022.

Where does the initial funding for the attack originate from?



(Diagram for Initial Funding)

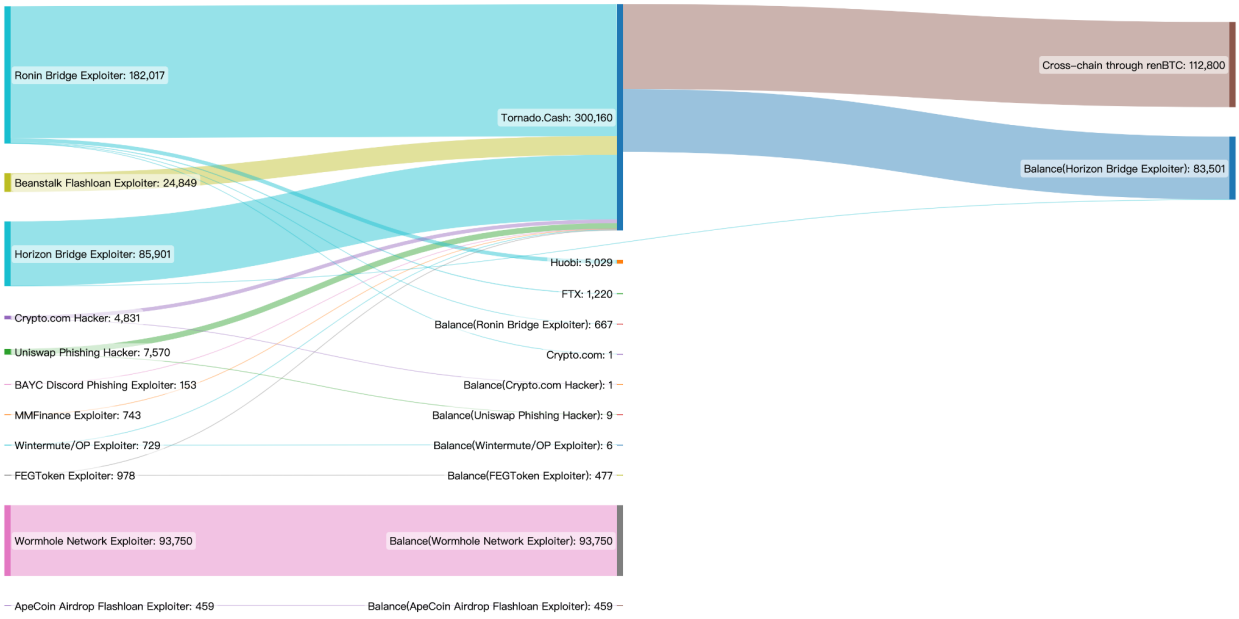
Tornado Cash accounts for the bulk of the initial funding for these security incidents. According to the diagram above, there have also been reports of withdrawals from exchanges, trading platforms, and personal wallets to fund these security incidents.

Where did the money that was laundered end up?

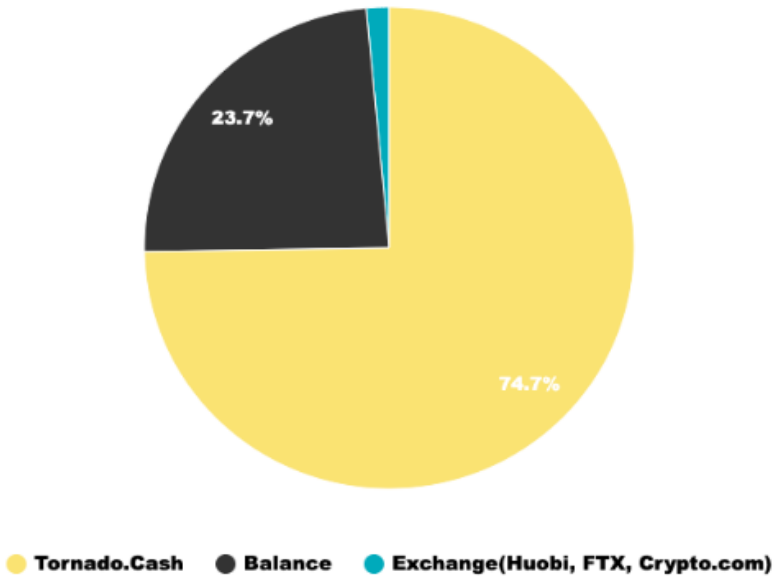
Based on our analysis of these security incidents, funds were laundered on the ETH or BTC blockchains. If the funds were not already on these two blockchains, hackers might consider moving them to these chains to continue the process.

The chart below was generated by analyzing the flow of ETH and BTC stolen during an incident.

- ETH Money Laundering Flow Chart



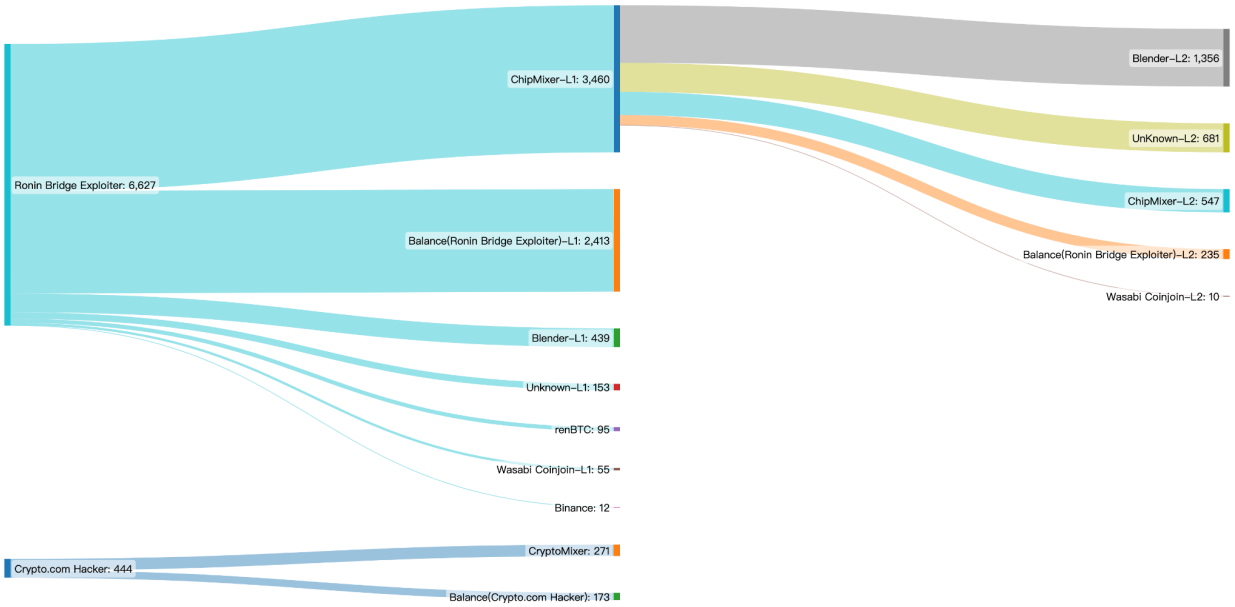
(ETH Money Laundering Flow Chart)



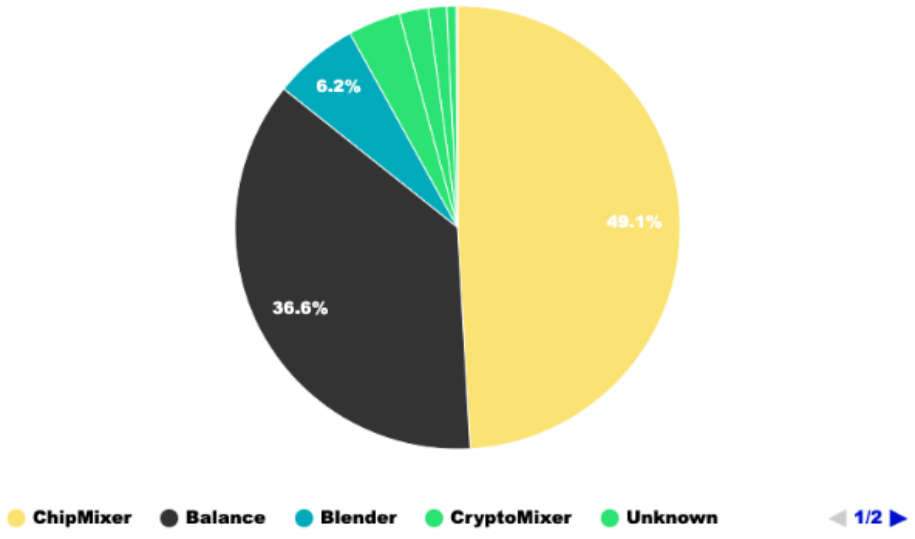
(Platform Percentage of ETH Laundered)

According to the flow chart, Tornado Cash receives 74.7% of the funds laundered on the ETH blockchain, up to 300,160 ETH. 23.7% of funds currently remain on the hacker's address, amounting to 95,570 ETH. 1.5% of the funds were sent to a trading platform, about 6,250 ETH.

- BTC Money Laundering Flow Chart



(BTC Money Laundering Flow Chart)



(Platform Percentage of BTC Laundered)

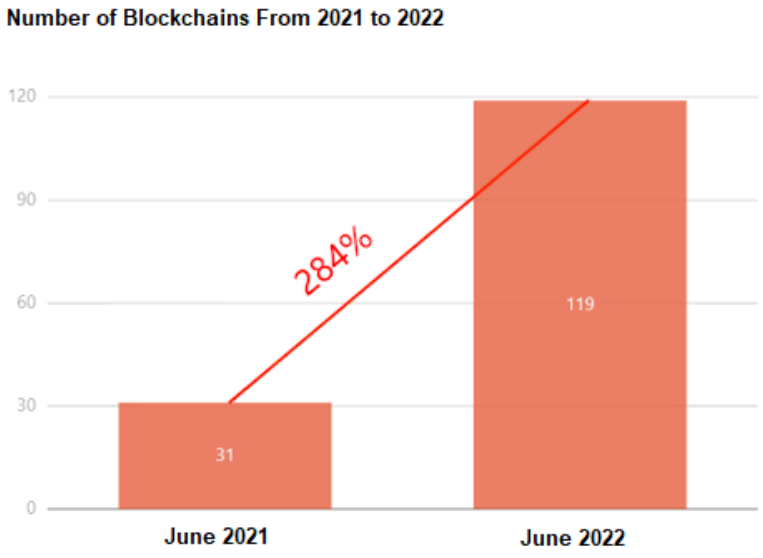
According to the chart above, 49.1% of funds laundered went to ChipMixer, totalling 3,460 BTC. 36.6% of laundered funds are currently held at the hacker's address, totalling 2,586 BTC. 6.2% of funds laundered were moved to Blender, with 3.8% of laundered funds moved to CryptoMixer and a small percentage to other unknown entities. 1.3% of laundered funds were moved to renBTC, 0.7% were moved to Wasabi Coinjoin, and 0.1% were moved to the Binance Exchange.

2. Current State of Blockchain Security

2.1 Overview of Blockchain Security

2.1.1 Blockchain Tracking

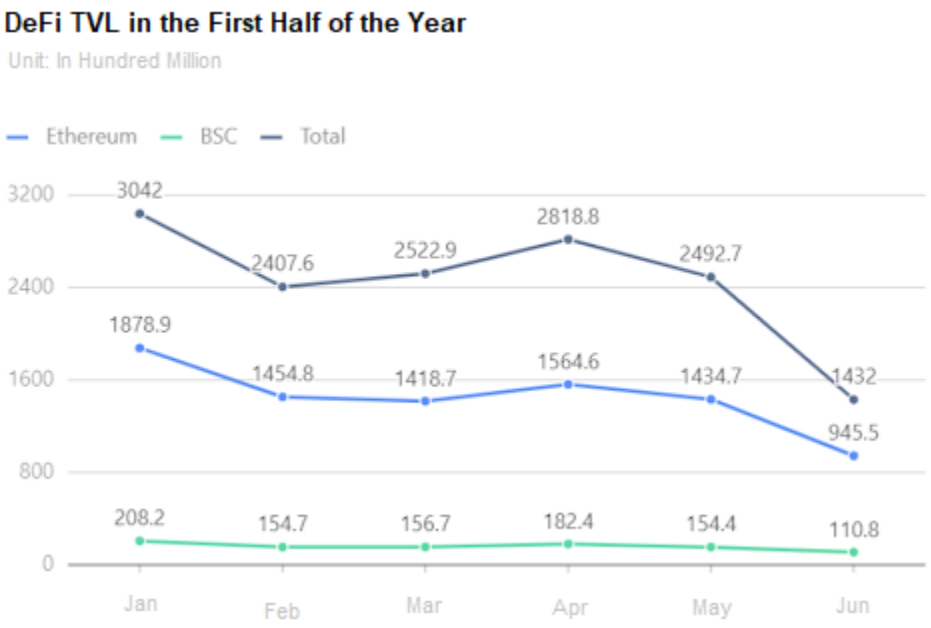
Blockchain continues to grow due to the emergence of NFT, DeFi, GameFi, and Metaverse. Simultaneously, these initiatives have boosted the growth and value of blockchains, bringing the multi-chain era closer to reality. According to Footprint Analytics data, the total number of blockchains out there as of June was 119, up from 31 in June 2021, representing a 284% rise year on year.



(Comparison of the number of Blockchains in June 2021 and June 2022)

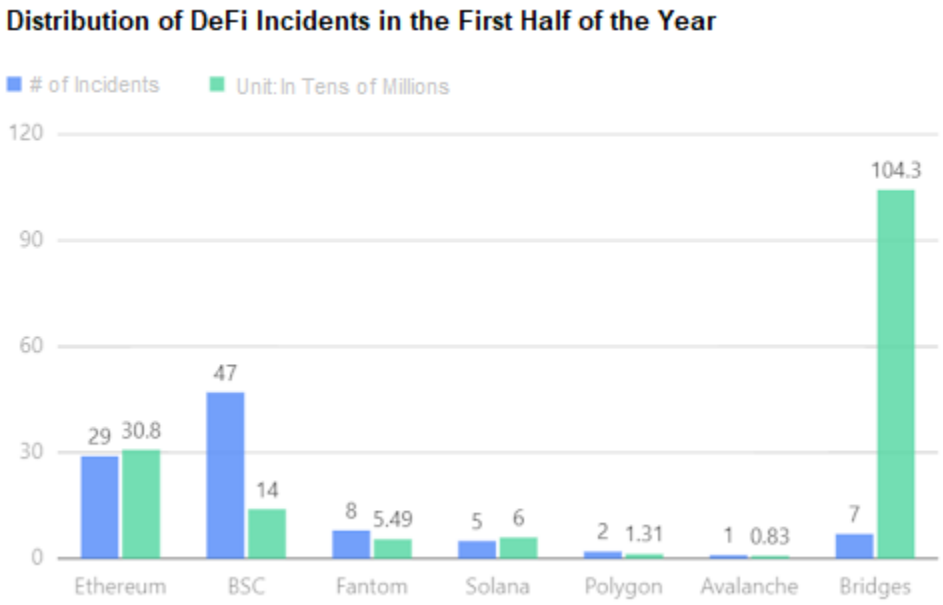
2.1.1.1 DeFi

According to DeFi Llama statistics, the total value locked (TVL) in DeFi on June 30 was $143.2 billion, with the ETH blockchain accounting for half of that, with TVL being $94.55 billion. Followed by the BSC with $11.08 billion. Since 2021, several emerging blockchains, such as Solana and Avalanche, have rapidly developed their on-chain ecosystems by integrating DeFi, therefore attracting a huge number of users and capital precipitation. On June 30, Solana had a TVL of $2.64 billion, up 77% from the previous year, where Avalanche had a TVL of $5.54 billion, up 96% from the previous year.



(2022 - DeFi TVL in the First Half of the Year)

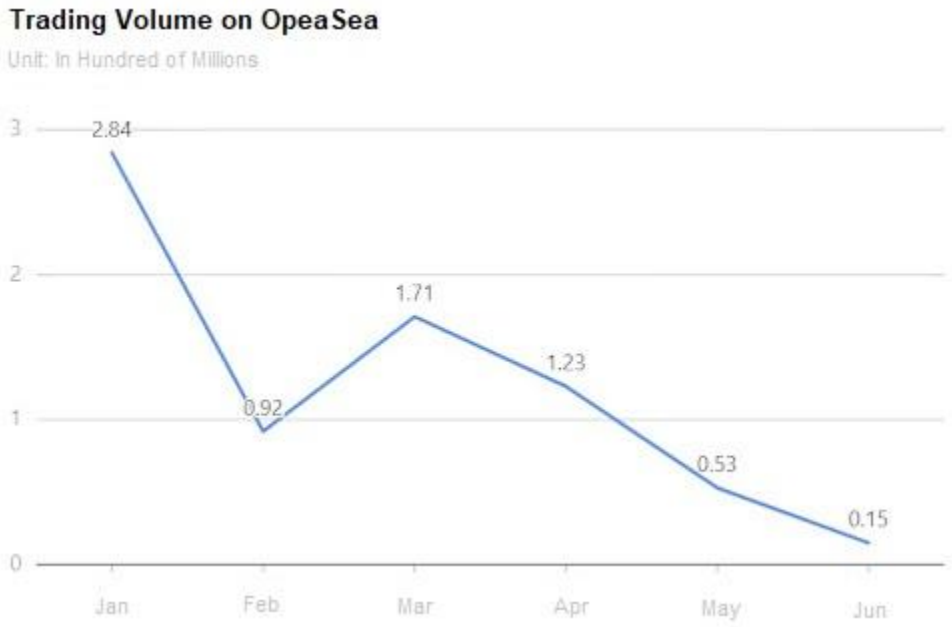
According to SlowMist Hacked, there were around 100 DeFi security incidents as of June 30, with damages exceeding $1.63 billion. The number of security incidents on BSC, ETH, Fantom, Solana, Polygon, Avalanche, and cross-chain bridges were 47, 29, 8, 5, 2, 1, and 7, respectively, with losses of $140 million, $308 million, $54.91 million, $63.83 million, $13.1 million, $8.3 million, and $1.043 billion respectively.



(2022 - Distribution of DeFi incidents in the First Half of the Year)

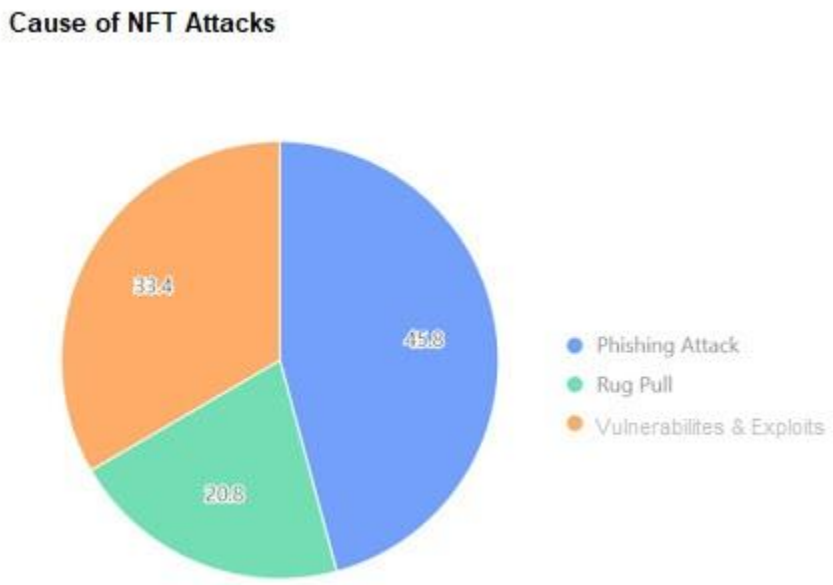
2.1.1.2 NFT

NFTs have grown fast as a result of the establishment of a number of leading NFT initiatives such as the involvement of celebrities and public figures. According to Dune Analytics, OpenSea's trading volume peaked in January at $284 million dollars, but with changes in the cryptocurrency market, OpenSea's trading volume in June was only $15.58 million dollars, a 94% decrease. The current NFT marketplace of the Ethereum ecosystem continues to dominate the market in terms of market capitalization and transaction volume, accounting for more than 90% of the total transaction volume. In addition to Ethereum, according to the statistics on transaction volume in the last 30 days, eco-friendly NFTs such as Solana and Flow are also growing at a rapid pace.



(2022 - Changes on OpenSea Trading Volume in First Half of the Year)

According to incomplete statistics from SlowMist Hacked data reports, there were about 48 NFT incidents as of June 30, with losses reaching up to $62.81 million dollars. Among them, 33.4% (16 incidents) were caused by attackers exploiting the project's own vulnerabilities. 20.8% (10 incidents) were caused by Rug Pull attacks, and phishing attacks accounted for 45.8% (22 incidents). The majority of which were caused by hackers posting phishing links on hacked media platforms such as Discord/Twitter.

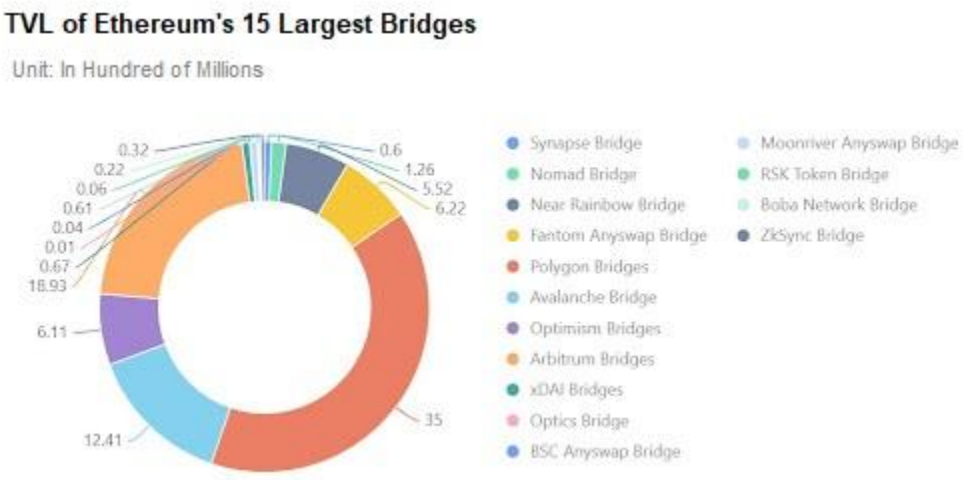


(2022 - Distribution of NFT Cause of Attack for First Half of the Year)

According to a TRM Labs report, in May and June, Chainabuse, a fraud reporting platform led by the TRM Labs community, received more than 100 reports of Discord hacking incidents. Since May, the NFT community has lost approximately $22 million. In June, hackers releasing NFT-related phishing attacks in compromised Discord channels rose by 55% this year.

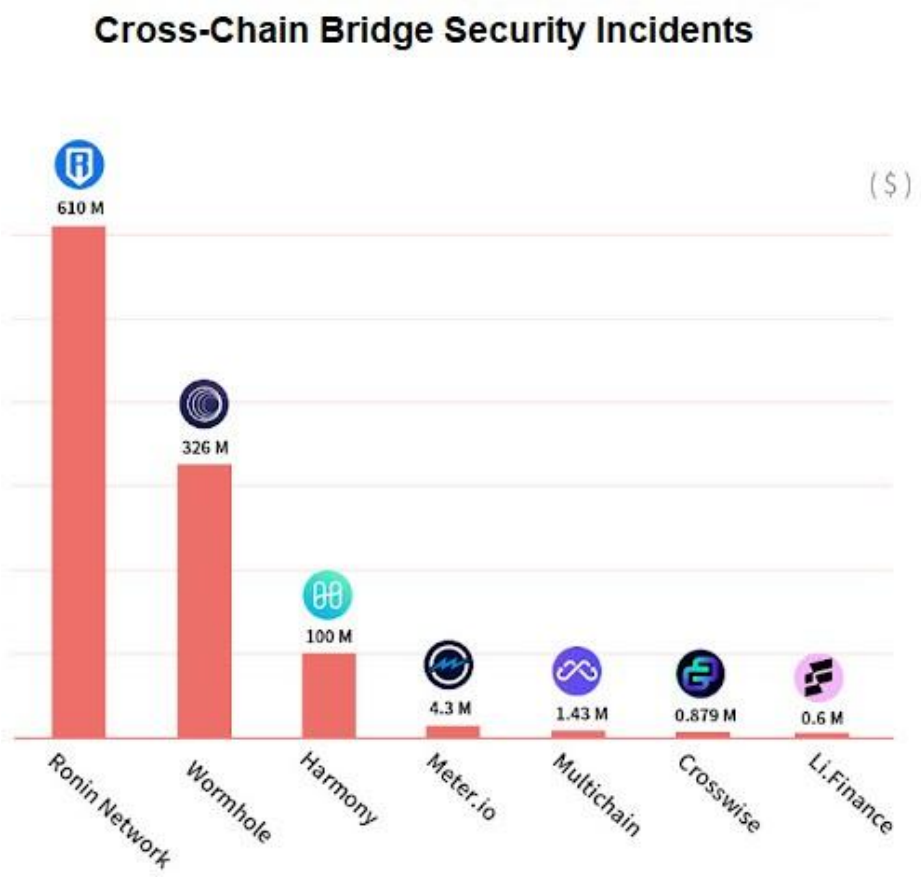
2.1.1.3 Cross-chain Bridges

With the advancement of blockchain technology, numerous chains now co-exist, with Ethereum serving as the foundation. Asset movement across chains and cross-chain interaction of smart contracts have become commonplace on the blockchain. According to the statistics by Dune Analytics, the total locked-in value (TVL) of Ethereum's 15 biggest cross-chain bridges was about $8.39 billion dollars as of June 30. Currently, the highest TVL is Polygon Bridges ($3.5 billion dollars), with the second largest being Arbitrum Bridge ($1.893 billion dollars), followed by Avalanche Bridge ($1.241 billion dollars).



(TVL of Ethereum's 15 Largest Bridges)

Because of the high quantity of liquidity and low degree of decentralization, multisig wallets hold practically all the power, and cross-chain bridges have also been deemed a "sweet spot" in the eyes of hackers. According to SlowMist Hacked data reports, as of June 30, there were seven cross-chain bridge security incidents, with losses totalling $1.043 billion, which accounts for 64% of DeFi's total losses and 53% of total losses overall in the first half of the year. It is worth mentioning that cross-chain bridges were involved in three of the four incidents that resulted in losses exceeding hundreds of millions of dollars in the first half of the year. Cross-chain bridges, as a crucial infrastructure of the multi-chain ecosystem, bear a large amount of capital flow and provide considerable ease to consumers. However, it poses numerous security and decentralization challenges, necessitating projects to increase its security, risk management, and other capabilities.



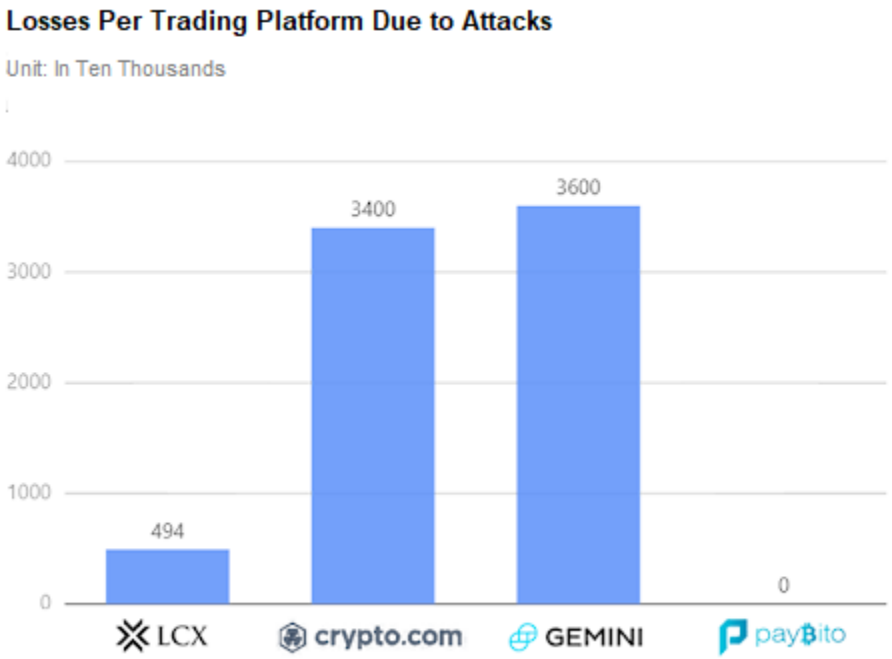
(2022 - Cross-chain Bridge Security Incidents in First Half of Year)

2.1.2 Trading Platforms

The cryptocurrency industry has been thrown into a regulatory whirlwind, with cryptocurrency trading platforms bearing the brunt of the damage. Using Binance as an example, the world's largest trading platform by volume, Binance has been exposed to regulatory warnings from dozens of countries and regions including Europe, the Americas, and Asia, since 2021. Binance has secured regulatory licenses and registered its platform in Spain, France, Abu Dhabi, Dubai, Italy, Bahrain, and other nations. In response to these significant global regulatory signals, Binance has gradually strengthened its compliance process. There were four trading platform security incidents worldwide in the first half of the year, with losses exceeding $77.7 million:

- The LCX technical team discovered unauthorized access to the LCX trading platform on January 9th, where roughly $7.94 million in crypto assets were stolen.

- Crypto.com. A small number of users had withdrawals made without their permission. They lost about $34 million dollars, which comprised 4,836.26 ETH, 443.93 BTC, and about $66,200 dollars in other cryptocurrencies.
- The LockBit ransomware group stated on January 8 that it had stolen a significant amount of customer information from the cryptocurrency trading platform PayBito.
- On January 12, the IRA Financial Trust, a pension account provider in South Dakota, USA, sued the cryptocurrency trading platform Gemini, stating that $36 million worth of crypto assets from a client's retirement account that Gemini was holding were stolen.



(2022 - Comparison of Attack Losses Per Trading Platform in First Half of the Year)

It is suggested that the largest trading platforms improve their internal management structure and technical processes. They should also make digital assets safer by putting in place security audit mechanisms, zero-trust mechanisms, and security solutions for both hot and cold assets.

2.1.3 Others

With the sudden rise in use of blockchain technology, it is inevitable that online dark web users will begin to consider it as an easy target. Criminals like how anonymous cryptocurrency is and have used it as a weapon of exploitation. Blockchain has become a new way for online black marketers to sell their goods. Extortion, fraud, and theft have become common in the blockchain ecosystem and pose a huge security risk.

According to data from the Payment System Department of the People's Bank of China, the use of cryptocurrency for payments will be second only to bank transfers as a way to make fraudulent payments in 2021, with amounts reaching $750 million. In 2020 and 2019, this number was only $130 million and $30 million respectively, but it is clear that this number will grow rapidly each year. The amount of cryptocurrency transfers in "pig butchering" scams has increased rapidly. The "pig butchering" scam funds paid out $139 million in cryptocurrencies in 2021, which is 5 times more than in 2020 and 25 times more than in 2019.

It is best for institutions and businesses to set up complete network security protection systems to protect against network security threats at all levels and ensure immediate delivery of alerts. When a security threat is detected, it can be dealt with quickly thanks to pre-emptive security intelligence.

Individual users can prevent the majority of risks by following the security rules and principles outlined below:

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:

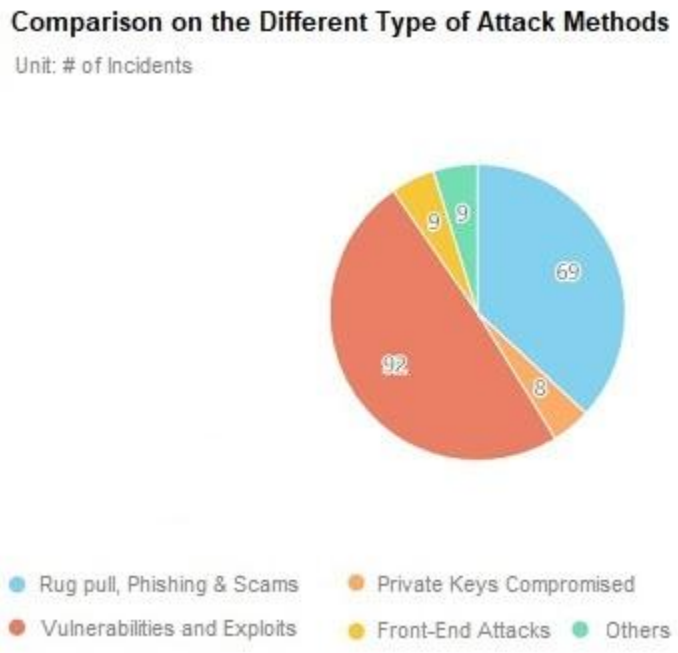
- For all the knowledge from the Internet, refer to at least two sources, corroborate each other, and always stay skeptical.

- 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 will make you regret afterwards.
- Pay attention to system security updates. Apply them as soon as they are available.
- Don't download & install programs recklessly can actually prevent most risks.

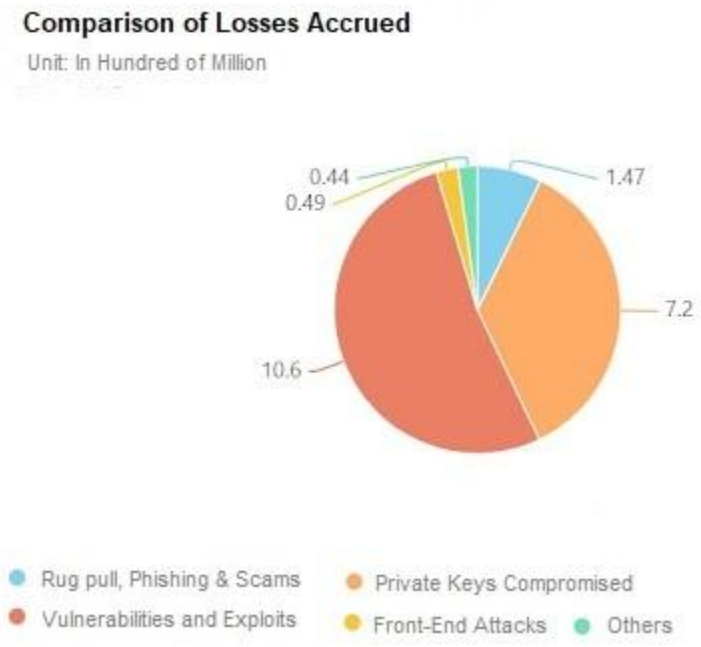
We strongly advised you to read and learn the "Blockchain Dark Forest Selfguard Handbook".

2.2 Overview of Attack Methods

Among the 187 security incidents, attack types are divided into four categories: the project's own design flaws, rug-pull and phishing scams, private key exposure, and the introduction of front-end malicious code. These four primary attack types account for 95% of all security issues.



(2022 - Comparison of the # of Attack Methods used in First Half of the Year)



(2022 - Comparison of Losses accrued per Attack Method in First Half of the Year)

92 attacks in the first half of the year were caused by the project's own design defects and numerous contract vulnerabilities, resulting in a loss of $1.06 billion. 19 of those attacks were caused by flash loans, which resulted in a loss of $61.33 million. The percentage of assets lost due to compromised private keys is approximately 4%, but the total loss is ~$720 million.

With the rapid development of Web3, attacks on users and developers, especially phishing attacks on media platforms such as Discord and Twitter have been on the rise. After acquiring administrator or account permissions, hackers typically disguise themselves as admins who end up launching these phishing links. Furthermore, the cost of producing these phishing websites is extremely low. By copying well-known NFT projects, users are lured into approving the transfer of their assets through the use of free or gifting NFTs. Rug Pull scams, on the other hand, are based on evil intentions of the project team. There were 42 Rug Pull incidents in the first half of the year, with the majority of them occurring on the BSC.

2.3 Known Security Incidents

This section outlines incidents from the first half of the year based on the following criteria: amount lost, occurrence frequency, scope of influence, and methodology.

2.3.1 Ronin Network $610 Million Loss

The Axie Infinity sidechain, Ronin Network, issued a community warning on March 29th regarding a security breach. A total of 173,600 ETH and 25.5 million USDC were stolen, totaling a $610 million loss. The attacker used compromised private keys to establish withdrawals and siphon funds from the Ronin bridge in just two transactions. Notably, the hack occurred on March 23, but officials allegedly discovered it after users reported that they were unable to withdraw 5,000 in ETH from the bridge. This incident's loss is even greater than last year's PolyNetwork hack, which lost over $600 million. The story begins in November of last year, when Sky Mavis asked Axie DAO for assistance in distributing free transactions. Due to the high volume of users, the Axie DAO whitelisted Sky Mavis, allowing Sky Mavis to sign various transactions on its behalf, a process that was discontinued in December. Access to the whitelist, on the other hand, was not revoked, allowing an attacker to sign from the Axie DAO validator via gas-free RPC once they gained access to Sky Mavis. The Sky Mavis' Ronin chain is made up of nine validating nodes, each of which requires at least five signatures to identify a deposit or withdrawal. The attackers discovered a backdoor via a gas-free RPC node, where they eventually gained control of five private keys, including Sky Mavis' four Ronin validators and an Axie DAO-run third-party validator. US investigators believe the incident was caused by the North Korean cybercrime organization, Lazarus Group.

2.3.2 Wormhole $326 Million Loss

On February 3, attackers used a signature verification vulnerability in the Wormhole network to generate 120,000 WETH, which was valued at $326 million on the Solana network. Wormhole's incident report stated that Wormhole's vulnerability in this incident was specifically an error in the signature verification code of the core Wormhole contract on the Solana side. This allowed attackers to forge messages to mint Wormhole's wETH, making this hack the largest in scale of losses on the Solana network to this day.

2.3.3 Beanstalk Farms Flashloan Attack

On April 17, Beanstalk Farms, an Ethereum-based algorithmic stablecoin project, was attacked, which resulted in a $182 million loss. The main reason for this attack was that there was no time interval between voting and proposal execution, which allowed the attacker to directly execute malicious proposals without community review after voting was over. Surprisingly, the attackers gave $250,000 of the money to an address used to collect donations for the Ukrainian government.

2.3.4 Harmony $100 Million Loss

The Harmony Horizon bridge was hacked on June 24. According to analysis by SlowMist's MistTrack platform, the attackers got away with more than $100 million USD, including 11 ERC20 tokens, 13,100 ETH, 5,000 BNB, and 640,000 BUSD. On the 26th, Harmony founder Stephen Tse stated on Twitter that Horizon was attacked due to a private key leak rather than a smart contract vulnerability. Despite the fact that Harmony encrypted their private keys, the attacker was able to decrypt some of them and managed to sign some unauthorized transactions.

2.3.5 Pokemoney Rug Pull Incident

A Rug Pull occurred on BSC on the NFT project, Pokemoney, where approximately 11,800 BNB (roughly $3.5 million) was stolen. The PokeMoney team claims the price drop was caused by an unexplained hack, even though no evidence of hacking was found. They claimed on Telegram that they couldn't access the project's Twitter account to inform the community regarding this incident.

2.3.6 Crypto.com Hacked Accounts

On January 17, 2022, Crypto.com learned that a small number of users had made unauthorized withdrawals of cryptocurrencies on their accounts, according to the Crypto.com investigation report. Crypto.com suspended all token withdrawals while maintaining basic operations. There were no financial losses among the clients. "We blocked unauthorized withdrawals in the majority of cases, and all other clients were fully reimbursed" stated Crypto.com. 483 Crypto.com users were affected by the incident. Unauthorized withdrawals totaled 4,836.26 ETH, 443.93 BTC and $66,200 in other currencies.

2.3.7 Uniswap Airdrop Phishing Attack

On July 12, Binance founder CZ tweeted that their security intelligence had detected a potential vulnerability in Uniswap V3 on the ETH blockchain. A few hours later, multiple Twitter users stated that there were no vulnerabilities with the protocol, but that it was a phishing attack. Over 70,000 addresses associated with Uniswap were airdropped malicious tokens. The airdrop directed users to a phishing site that looked identical to the real Uniswap site. Users were duped into signing contracts that allowed the attackers to take over their wallets and steal their funds and NFTs. One wallet lost more than $6.5 million in cryptocurrency, while another lost about $1.68 million.

2.3.8 OpenSea E-mail Phishing Scams

The world's largest NFT marketplace, OpenSea, was attacked on February 20. According to an official tweet from OpenSea, hackers sent phishing emails to all users' mailboxes at the same time the OpenSea contract was upgraded. Many users mistook it for an official email and authorized their wallets, which resulted in their assets being stolen.

2.3.9 ApeCoin Flashloan Arbitrage

According to Twitter user Will Sheehan, on March 17, an arbitrage bot took out more than 60k in ApeCoins (worth $8 each) via flash loans. An investigation revealed that this was due to a flaw in ApeCoin's airdrop mechanism. ApeCoin airdrops are determined by whether a user has the instantaneous state of BYAC NFT, which attackers can manipulate via flash loans. The attacker first borrowed BYAC via a flash loan and used these NFTs to claim the airdropped APE tokens. The attacker then returned the flash loan.

2.3.10 BAYC Official Discord Hack

BAYC announced on its official Twitter on June 5 that its Discord server was briefly attacked and NFTs worth approximately 200 ETH were stolen. The attack was carried out by a compromised account of a community administrator, who posted a link to a phishing site.

2.3.11 FEG - 2 Flashloan Attacks

A flash loan was used to attack the multi-chain DeFi protocol FEG on May 16. The attackers stole 144 ETH and 3,280 BNB, totaling approximately $1.3 million. On May 17th, FEG was attacked again, where this time the attackers stole 291 ETH and 4,343 BNB, totaling $1.9 million, with $1.3 million on the BSC and $600,000 on the ETH blockchain. While both attacks are similar, the main reason is that the path address parameter in the swapToSwap function was not verified, allowing the attacker to arbitrarily pass in the malicious path address, which caused the FEGexPRO contract to authorize the attacker's own tokens.

2.3.12 Optimism 20 Million $OP Lost due to Loopholes

On June 9, both Optimism and Wintermute issued announcements informing the community of the loss of 20 million OP tokens. Optimism entrusted Wintermute to provide liquidity services for OP tokens in the secondary market at the time of their release, where Optimism would provide Wintermute with 20 million OP tokens. Wintermute provided a multi-signature address to which Optimism transferred 20 million OPs after testing two transactions confirmed by Wintermute. Wintermute discovered that they had no control over the coins after Optimism transferred them because the multi-signature addresses they provided were only deployed on the Ethereum mainnet for the time being and had not yet been deployed to the Optimism network. Wintermute immediately began remediation operations in order to gain control of these tokens. However, attackers were already aware of this flaw and deployed the multi-signature address on the Optimism network prior to Wintermute, successfully controlling the 20 million tokens. At the moment, the Optimism hacker has returned 17 million OP tokens and transferred 1 million OP to Vitalik's address.

2.3.13 MM.finance DNS Hijacking Attack

The MM.finance website was hit by a DNS attack on May 4. According to an official document, the attacker was able to inject malicious contract addresses into the front-end code. The attacker used a DNS vulnerability to change the router contract address in the escrow file. More than $2 million in cryptocurrency assets were stolen and transferred to the ETH blockchain via the use of a bridge. The attacker then laundered the funds via Tornado Cash.

2.3.14 KLAYswap Malicious Front-End Attack

KLAYswap, a South Korean DeFi project, announced on February 3 that it had been hacked and had lost approximately 2.2 billion won, or approximately $1.83 million. According to the announcement, hackers tampered with third-party JS links on the front end of KLAYswap via BGP hijacking. This infected users when they accessed the KLAYswap page and then authorized assets to be transferred to the hacker's wallet address. During that time, 325 wallets experienced 407 transactions.

2.3.15 Terra Ecosystem Collapse

On May 9th, Terra's algorithm backed stablecoin UST was severely de-pegged, turning LUNA's value into virtually nothing. Tens of billions of dollars in market value vanished overnight. The Luna Foundation Guard (LFG) attempted to keep the value of UST stable by spending approximately $3.5 billion in Bitcoin. Terra eventually ceased operations on May 12. Terra's debacle resulted in a $60 billion loss, which created a sell-pressure effect on Bitcoin's price and spread fear throughout the crypto industry.

3. Anti-Money Laundering Analysis of Security Incidents

With regards to our AML analysis of these incidents, we'll be covering the following topics:

- Providing a method for analyzing outgoing transactions from mixers such as Tornado Cash and ChipMixer
- Utilizing anti-money laundering techniques to examine security incidents

3.1 Overview of security incident losses

We will be using the incidents listed above for our AML analysis:

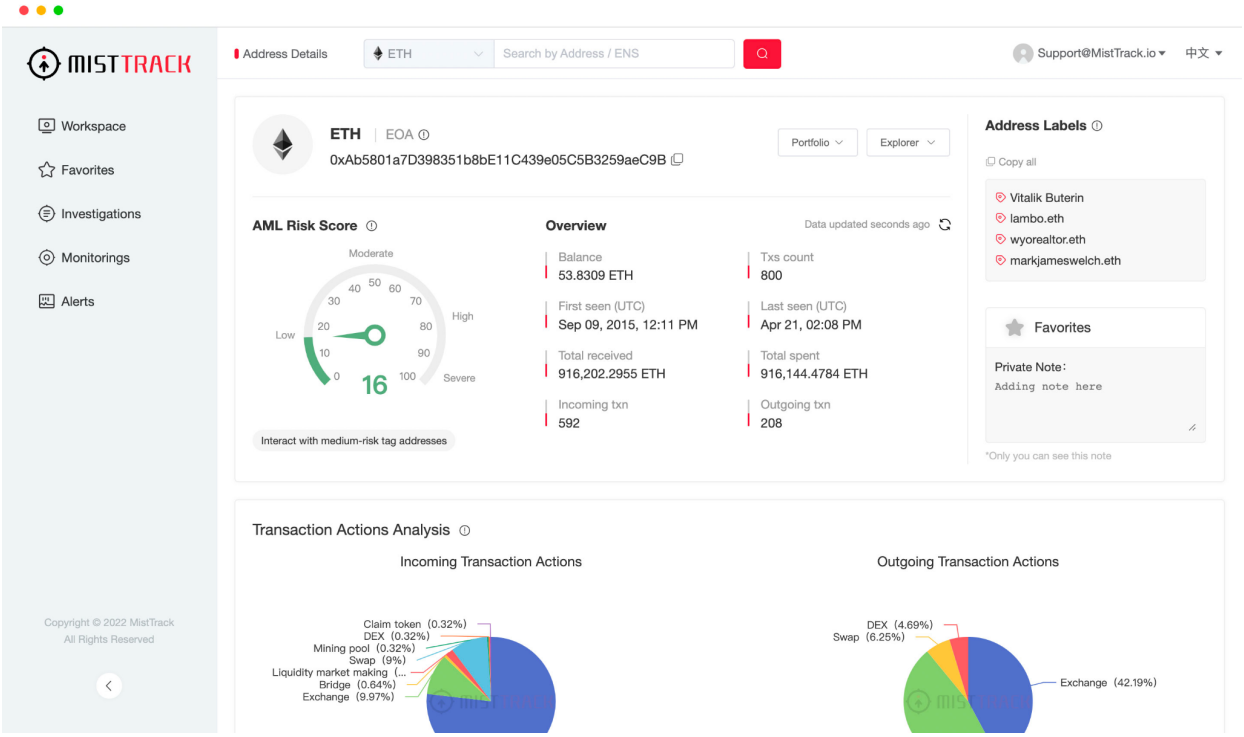
Event	Date Stolen	Amount Lost
Ronin Network	March 23, 2022	173,600 ETH、25,500,000 USDC

Wormhole	February 2, 2022	120,000 WETH
Beanstalk	April 17, 2022	24,830 ETH、250,000 USDC Tokens and 36,390,000 BEAN Token
Harmony	June 23, 2022	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 and 5,620,000 FRAX BSC ：5,000 BNB and 640,000 BUSD
Crypto.com	January 17, 2022	ETH：4,836.25 ETH BTC：443.93 BTC
Uniswap Phishing	July 11, 2022	3,278.84 ETH and 240.42 WBTC
ApeCoin Airdrop Flashloan Arbitrage	March 17, 2022	60,564 APE
BAYC Official Discord Hacking	June 4, 2022	Approximately 145 ETH ($256,000) of NFTs
FEGToken	May 15 & 16, 2022	443.86 ETH and 7,626.49 BNB
Optimism	May 27, 2022	20,000,000 OP Tokens (17,000,000 OP returned)
MM.finance	May 4, 2022	$2,000,000

3.2 Tools & Methods Used

Before starting our investigations, we must first have an efficient tool and a suite of analytical approaches to effectively analyze complex money laundering techniques.

3.2.1 Basic Tools- MistTrack



(MistTrack - Example Diagram of Anti-Money Laundering Tracking System)

MistTrack was designed by SlowMist as a crypto analytics platform that combines a number of SaaS systems. It was specifically designed to target crypto money laundering activities. Our core functions include AML Risk Scores, Transaction Analysis, Asset Tracing, and Monitoring.

- **AML Risk Score**

The AML risk score is a score assigned to an address owner by analyzing its historical transaction data against SlowMist's database of malicious wallets. If an address belongs to a high-risk entity,

such as a mixer, or if it received cash from it, it will be assigned a high risk score. Any confirmed addresses involved in illicit activities such as extortion, theft, phishing, and/or fraud are automatically marked as risky in SlowMist's database.

- **Address Labels**

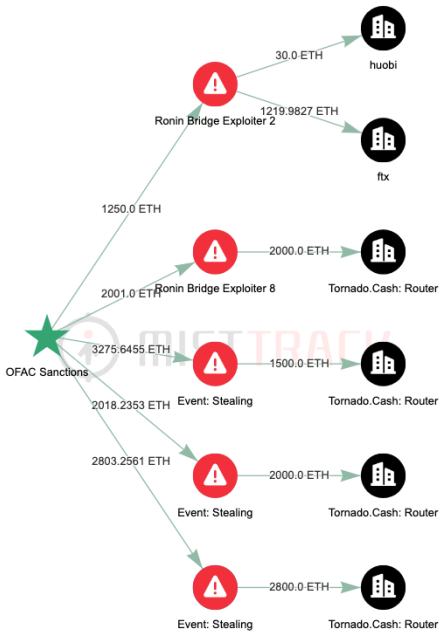
The MistTrack database has accumulated over 200 million wallet addresses. These address include information based on the following 3 categories:

1. Entity addresses such as Coinbase, Binance, etc.
2. On-chain analytics on DeFi whales, MEV Bots, and ENS.
3. Off-chain data, such as imToken/MetaMask wallets users.

- **Investigations**

MistTrack plays a crucial part in the analysis and evaluation of anti-money laundering through its analysis of transaction characteristics, on-chain activities, and capacity to monitor any wallet address.

Our investigation feature allows users to track and visualize the flow of crypto assets between wallets. Users can also monitor the movements of funds in real time. All information, on-chain and off-chain, are integrated into one panel to provide a complete analysis that can be turned over to law enforcement agencies as evidence.



(MistTrack - Example Diagram of Tracking Analysis)

Our database has over 1,000 entity addresses, 100,000 threat intelligence addresses, 90 million malicious activity addresses, and has tagged over 200 million addresses. This is to provide users with a comprehensive database for anti-money laundering research and analysis.

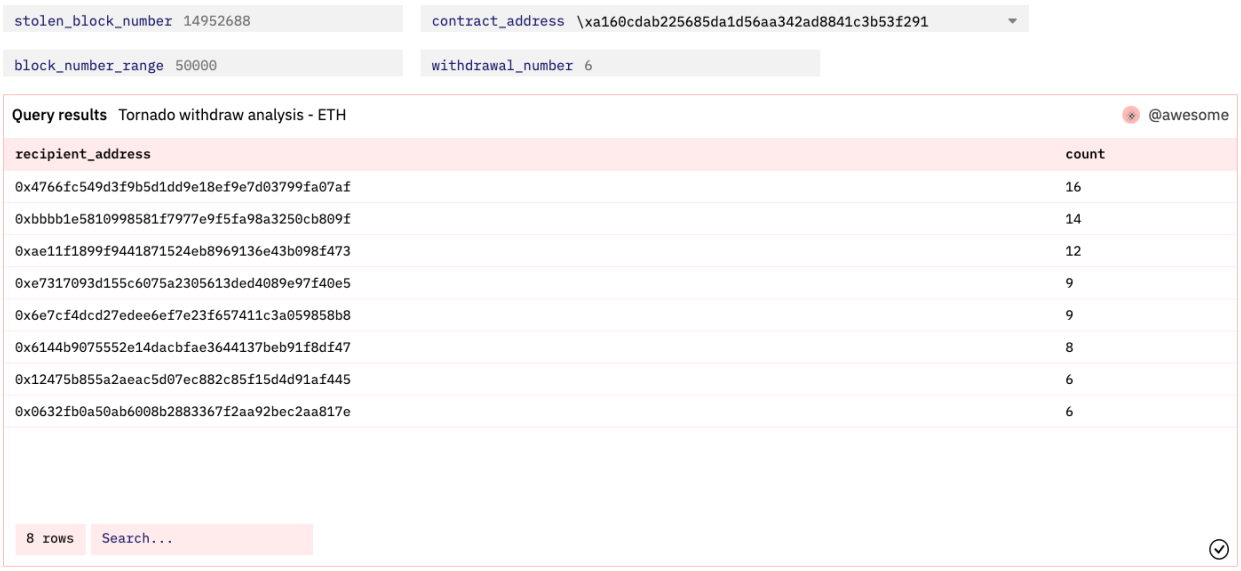
3.2.2 Extended Methods - Data Analysis

We can see from a number of incidents that stolen funds on the ETH/BSC chain have typically been transferred to mixers such as Tornado Cash, making it the platform of choice for scammers and hackers to launder their funds. While MistTrack is effective for conventional AML analysis, additional resources are required for more complex cases.

New laundering techniques necessitate the development of new analytical processes including the analysis of Tornado Cash transactions. Here we will discuss one of the methods we use for analyzing transfers out of Tornado Cash.

- First, we'll make a note of what information we know currently, such as the total number of transfers, the time of the initial deposit, and the block height of the first deposit.

- Then, we fill in the parameters in the Dune dashboard we've prepared.
- We'll obtain preliminary withdrawal data and then further filter the results using the feature classification method.
- Following a screening, the addresses that's most likely to be associated with the scammer will be provided and the result set with the highest probability is selected and verified.



stolen_block_number 14952688

contract_address \xa160cdab225685da1d56aa342ad8841c3b53f291

block_number_range 50000

withdrawal_number 6

Query results Tornado withdraw analysis - ETH @awesome

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

8 rows Search...

(Dune Dashboard - Tornado Cash Withdrawal Analysis)

Through this technique, we were able to correctly identify the withdrawal address of stolen funds from numerous incidents such as the Ronin network exploiter.

Evidently, this strategy has some limitations:
A parameter is the amount of funds sent to Tornado Cash. The amount of anonymity set decreases as the amount of funding increases. The opposite is true when lesser funds are sent. As a result, it is more challenging to analyze small sums sent to tornado cash.

On the Bitcoin network, ChipMixer and Blender are platforms frequently utilized for laundering by malicious actors. Blender is currently sanctioned by the United States Treasury; hence, the website is no longer accessible and will not be addressed further.

Due to the substantial influx of funds via ChipMixer, we have also proposed a method for analyzing their transactions.

- We identify ChipMixer's withdrawal characteristics.

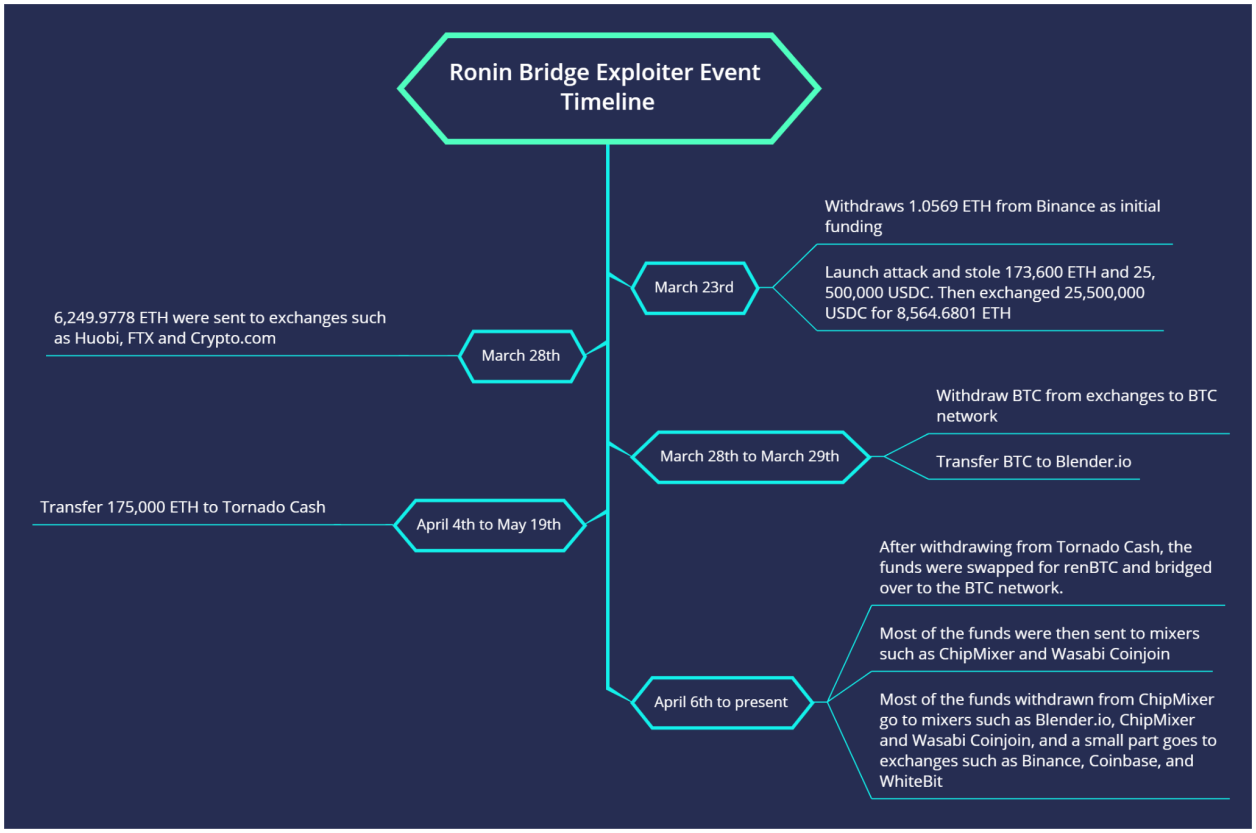
Entry Address Type	Output Address Type	Amount Entered	Version	Lock Time
bech32(bc1q...)	bech32(bc1q...)	All input amounts meet the requirement of Chips (i.e. 0.001 * 2 to the nth power, n < 14)	2	Block Height - 1 Block Height - 2 Block Height - 3

- We then scan and filter the structured block data for the relevant time period based on the aforementioned withdrawal characteristics. Then we collect ChipMixer's withdrawal records within this time frame.
- We categorize the withdrawal data and verify the results with the highest probability.

3.3 Detailed AML Analysis

3.3.1 Ronin Network

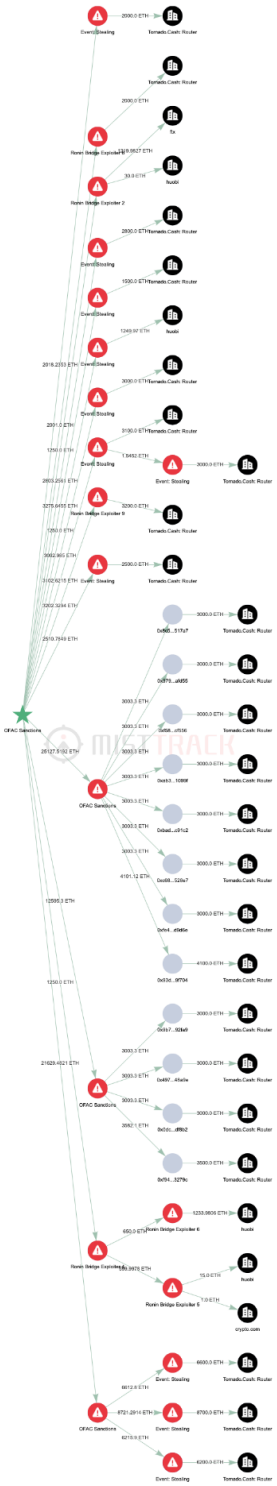
Hacker address: 0x098B716B8Aaf21512996dC57EB0615e2383E2f96 (ETH)
Date: 03/23/2022
Amount: 173,600 ETH, 25,500,000 USDC
Initial funding: SimpleSwap
Event:



(Ronin Bridge Exploiter - Timeline of Fund Transfers)

ETH Transfer

The hacker exchanged the 25,500,000 USDC from the attack to 8,562.6801 ETH, bringing the total amount needed to launder to 182,163.737 ETH (Binance withdrawal 1.0569 ETH + stolen 173,600 ETH + exchange from USDC 8,562.6801 ETH).



(Ronin Bridge Exploiter - Diagram of Funds Transferred)

Transfer Chart:

Platform	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 funds not account were lost during the laundering process

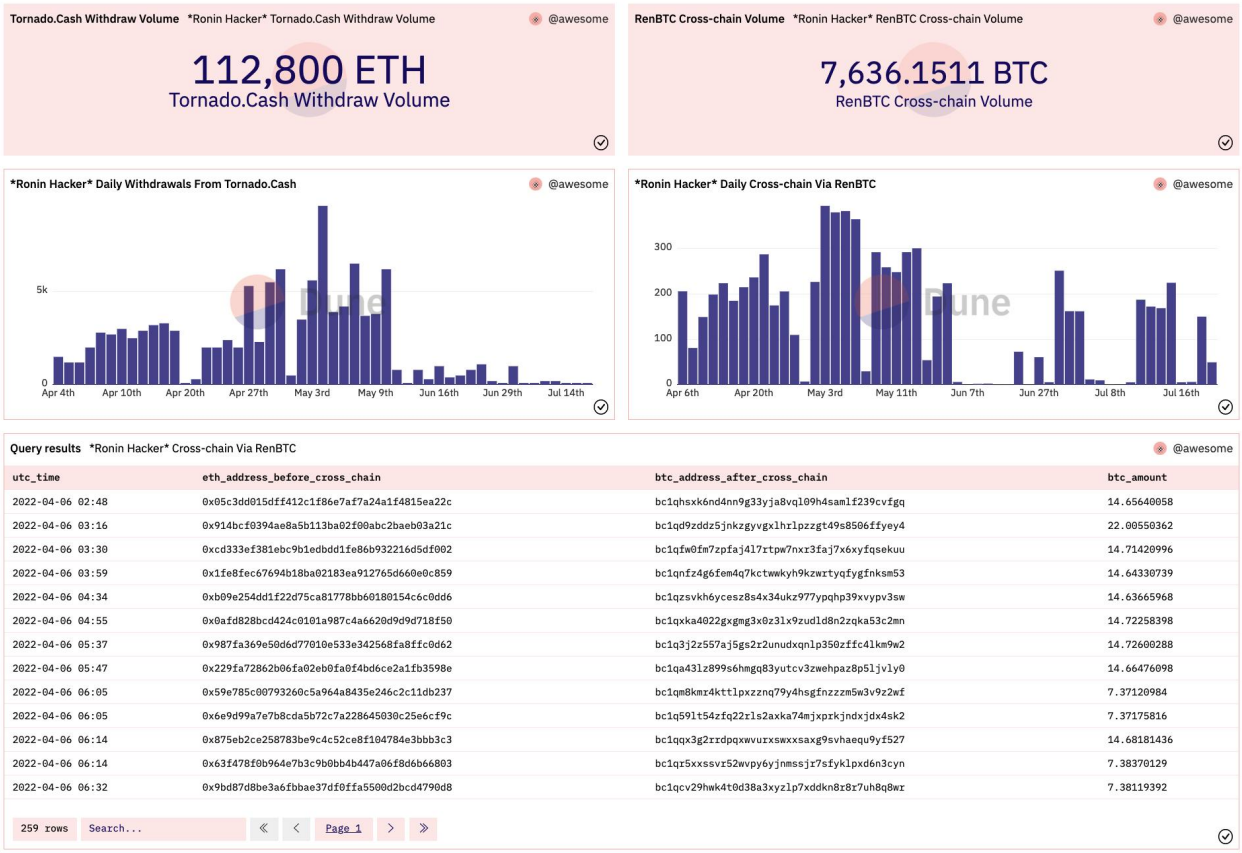
Tornado Cash Transfer:

The hacker transferred a total of 175,100 ETH to Tornado Cash. After our analysis, we concluded that the Ronin hacker's withdrawal from Tornado Cash had the following characteristics.

After withdrawing from Tornado Cash, the hacker used 1inch & Uniswap to exchange the funds for renBTC before finally bridging it to the Bitcoin network.

Using Dune Analytics, we filtered out data pertaining to Tornado Cash withdrawals and funds that were moved to the Bitcoin network that matched the criteria above.

This process is illustrated below:



(Ronin Hacker from Tornado Cash Cross-chain data of renBTC after transfer)

Transfer Chart:

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

Note. Data is valid up to July 20. 2022

BTC Transfer

Based on our analysis, a total of 8,075.9329 BTC met the criteria using the method above. Among them, 6,191.2542 BTC were possibly associated with the Ronin hacker, coupled with the 439.7818 BTC that was withdrawn from Huobi and FTX. A total of 6,631.036 BTC had possible connections to the Ronin hacker.

Additional details provided below:

Platform Used	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 aren't accounted for,

ChipMixer Transfer

According to the transfer of BTC, it can be seen that 3460.6845 BTC was transferred to ChipMixer. By combining on-chain data along with the analysis of ChipMixer's withdrawal data, we were able to determine that the Ronin hackers withdrew a total of 2,871.03 BTC through ChipMixer.

Details below:

Platform	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 aren't accounted for.

3.3.2 Wormhole

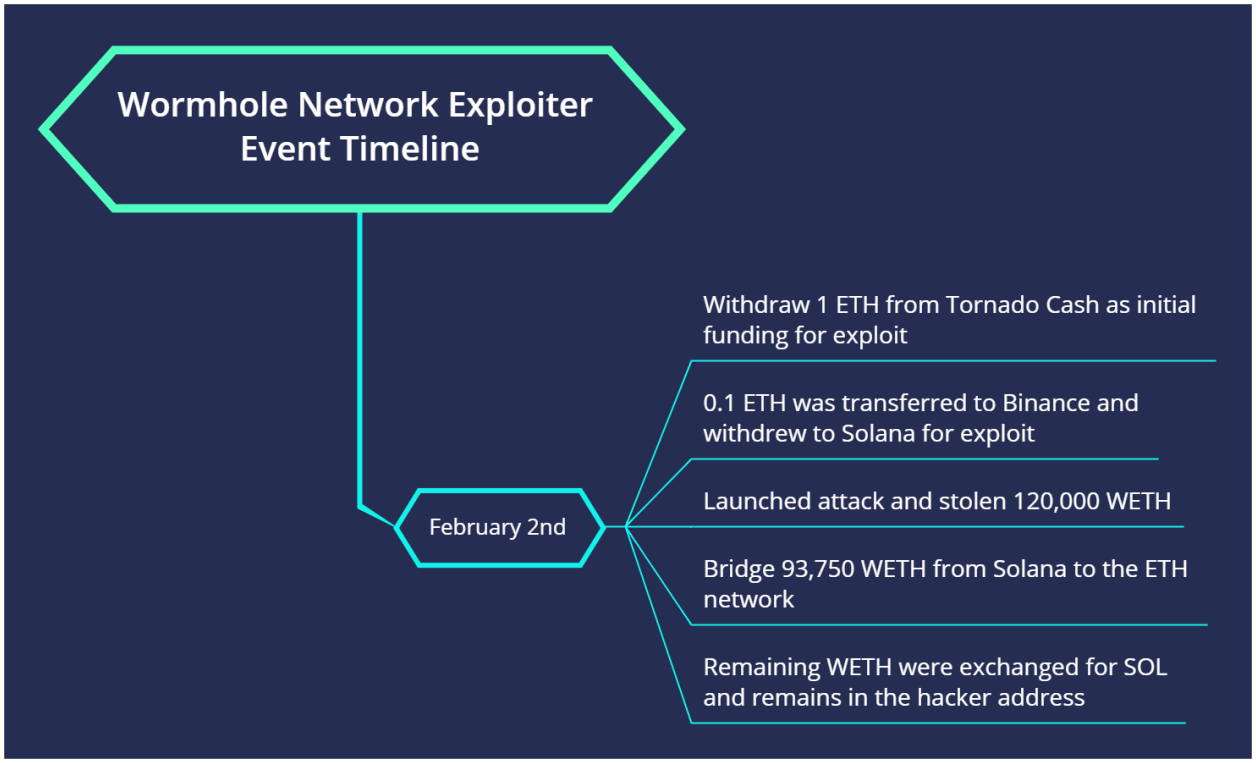
Hackers Address: CxegPrfn2ge5dNiQberUrQJkHCcimeR4VXkeawcFBBka (Solana)

Date: 02/02/2022

Amount stolen: 120,000 WETH

Initial funding: Tornado Cash

Events:



(Wormhole Network Exploiter - Timeline of Fund Transfers)

WETH Transfer Chart:

Transfer Method	Funds Transferred
Bridge to ETH blockchain	93,750 WETH
Conversion to SOL	26,250 WETH

Balance of Hackers Address:

Addresses	Balance of
CxegPrfn2ge5dNiQberUrQJkHCcimeR4VXkeawcFBBka	432,661.15 SOL
0x629e7da20197a5429d30da36e77d06cdf796b71a	93,750.623 ETH

3.3.3 Beanstalk

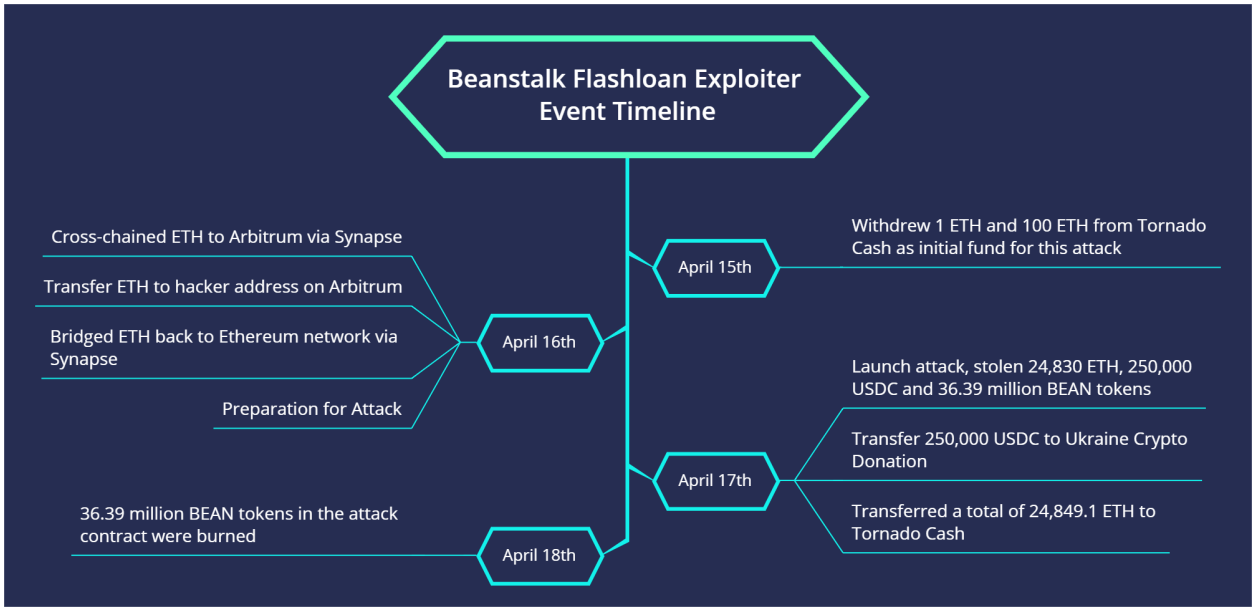
Hackers Address: 0x1c5dCdd006EA78a7E4783f9e6021C32935a10fb4 (ETH)

Date: 04/17/2022

Amount: 24,830 ETH, 250,000 USDC, 36,390,000 BEAN

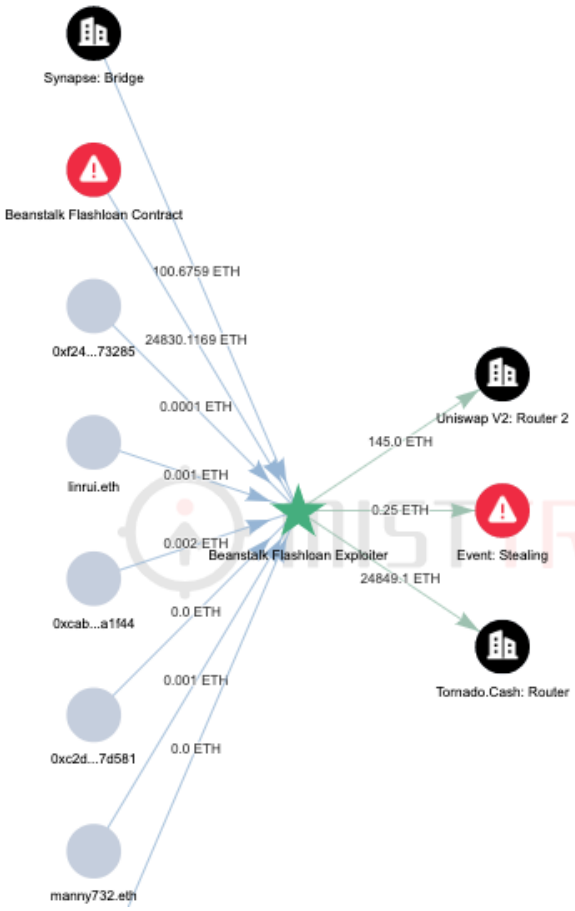
Initial funding: Tornado Cash

Events:



(Beanstalk Flashloan Exploiter - Timeline of Fund Transfers)

ETH Transfer



(Beanstalk Flashloan Exploiter ETH - Diagram of Funds Transferred)

ETH Transfer Chart:

Transfer Method	Funds Transferred
Tornado.Cash	24849.1 ETH

Note: The transfer funds include the remaining funds of the attack fee.

3.3.4 Harmony

Hackers Addresses:

0x0d043128146654C7683Fbf30ac98D7B2285DeD00 (ETH)

0x0d043128146654C7683Fbf30ac98D7B2285DeD00 (BSC)

Date: 06/23/2022

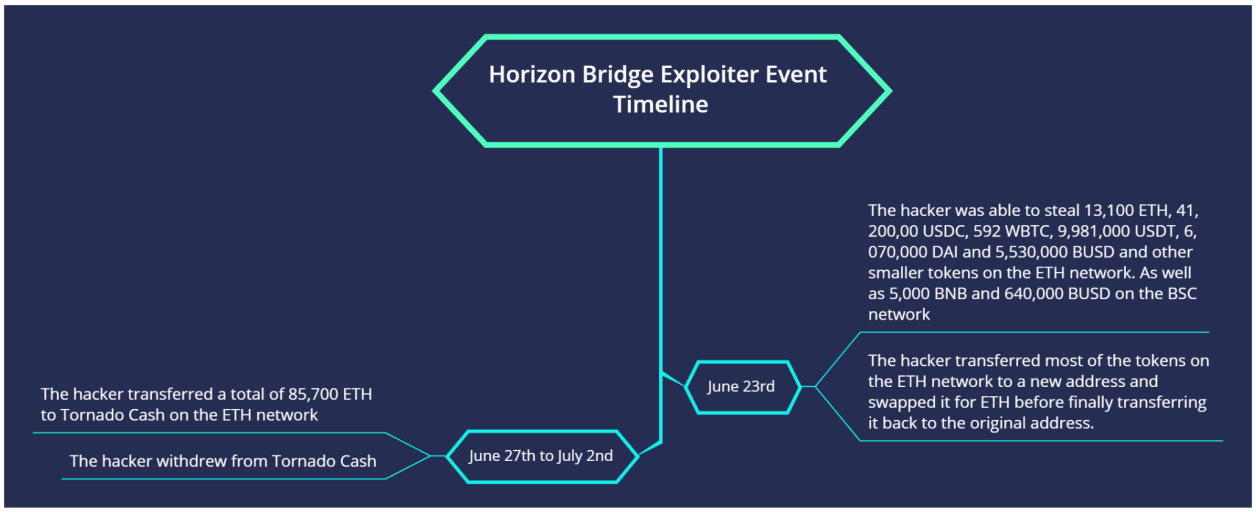
Amount:

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

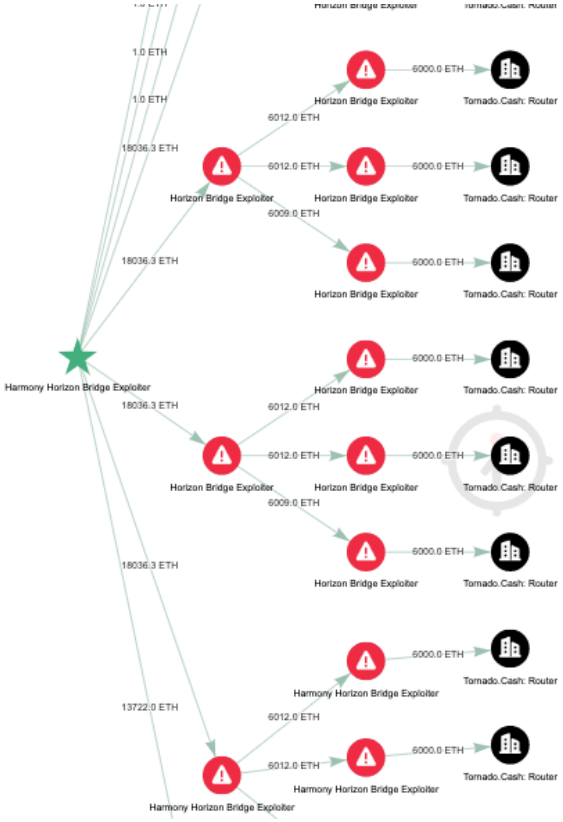
Initial Funding: N/A

Events:



(Horizon Bridge Exploiter - Timeline of Fund Transfers)

ETH Transfer



(Horizon Bridge Exploiter ETH - Diagram of Funds Transferred)

ETH Transfer Chart：

Transfer Method	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.

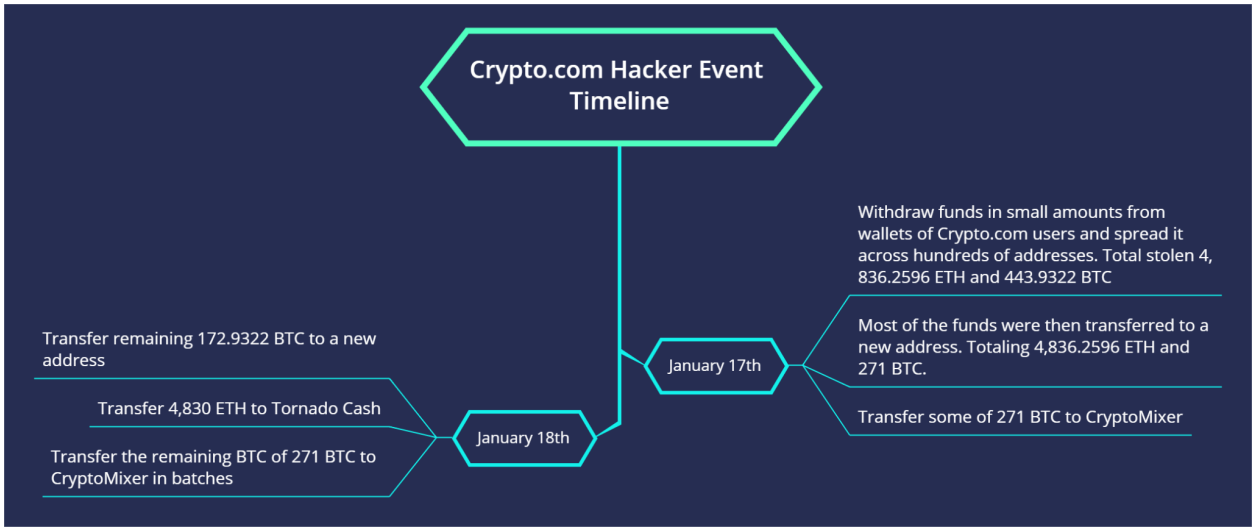
According to the Tornado Cash withdrawal characteristics provided above, a total of 83,300 ETH withdrawals had ties to the hackers.

ETH Transfer Chart:

Transfer Direction	Funds Transferred
Tornado Cash	83,300 ETH

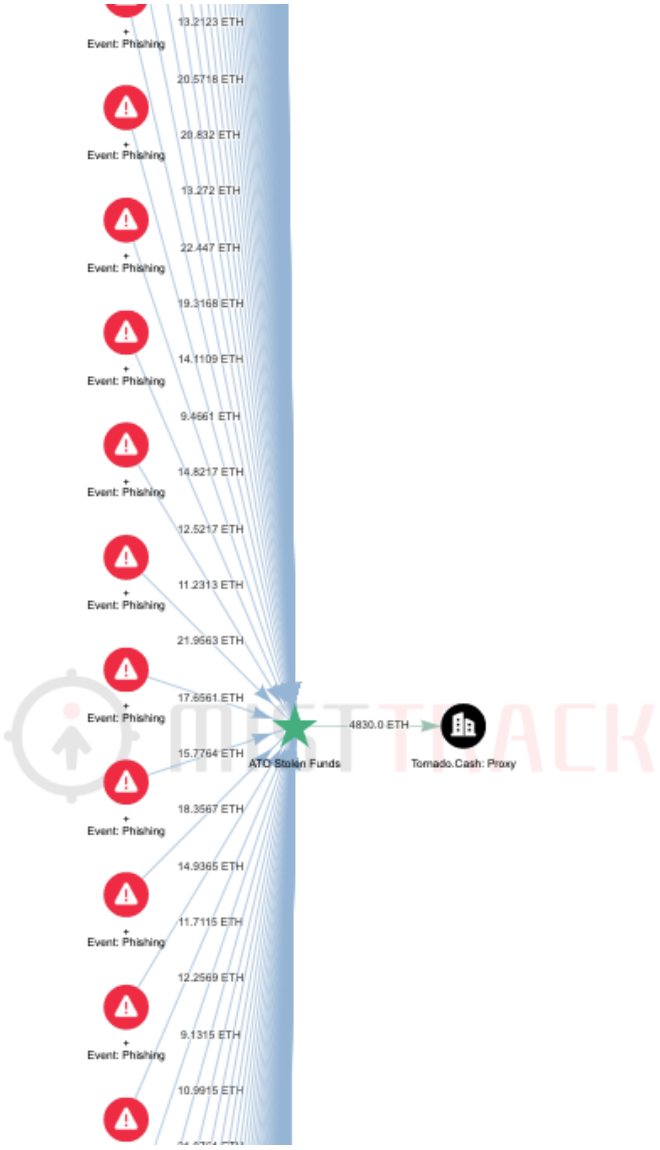
3.3.5 Crypto.com

Hackers Addresses:
0x6e1218c55f1aCb588Fc5E55B721f1183D7D29D3d (ETH)
bc1qk8wlwypvvr6v5lmsngg5a248k2a9cgrsrw5jsq (BTC)
bc1q83c9e7s8925hhy9dzqpdyyfctgwaspj3wdrhqr (BTC)
bc1qk7e2k8s252789cggr5xy67m6jvc0jsqpdjfw9d (BTC)
bc1qnzn9wmt40qwuhd7zmqvmvd0c3zazv59ljplrnr (BTC)
bc1qy7hf94vv20jqez2fk8xyxuv0h0u8r0kh8cau46 (BTC)
Date: 01/17/2022, 01/18/2022
Amount: 4,836.2596 ETH, 443.9322 BTC
Initial Funding: N/A
Flow of Transfers:



(Crypto.com Hacker - Timeline of Fund Transfers)

ETH Transfer



(Crypto.com Hacker ETH - Diagram of Funds Transferred)

ETH Transfer Chart:

Transfer Method	Funds Transferred
Tornado.Cash	4,830 ETH
Balance	1.1692 ETH

BTC Transfer

BTC Transfer Chart：

Transfer Method	Funds Transferred
CryptoMixer	271 BTC
Balance	172.9322 BTC

3.3.6 Uniswap Phishing

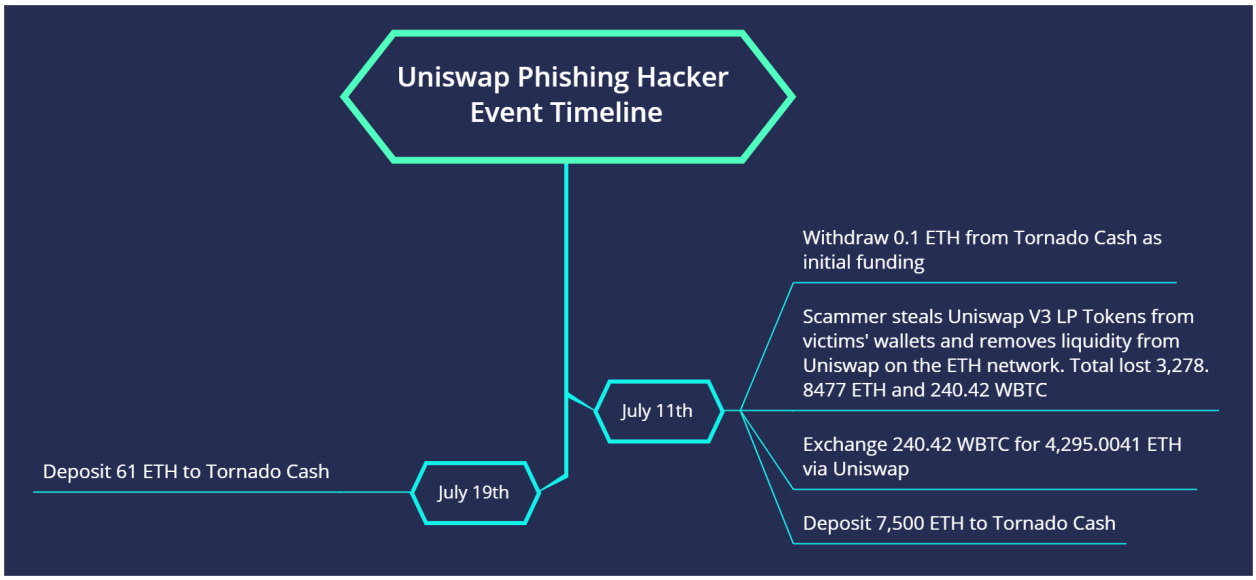
Hackers Address: 0x09b5027ef3a3b7332ee90321e558bad9c4447afa (ETH)

Date: 07/11/20227

Amount: 3,278.8477 ETH, 240.42 WBTC

Initial Funding: Tornado.Cash

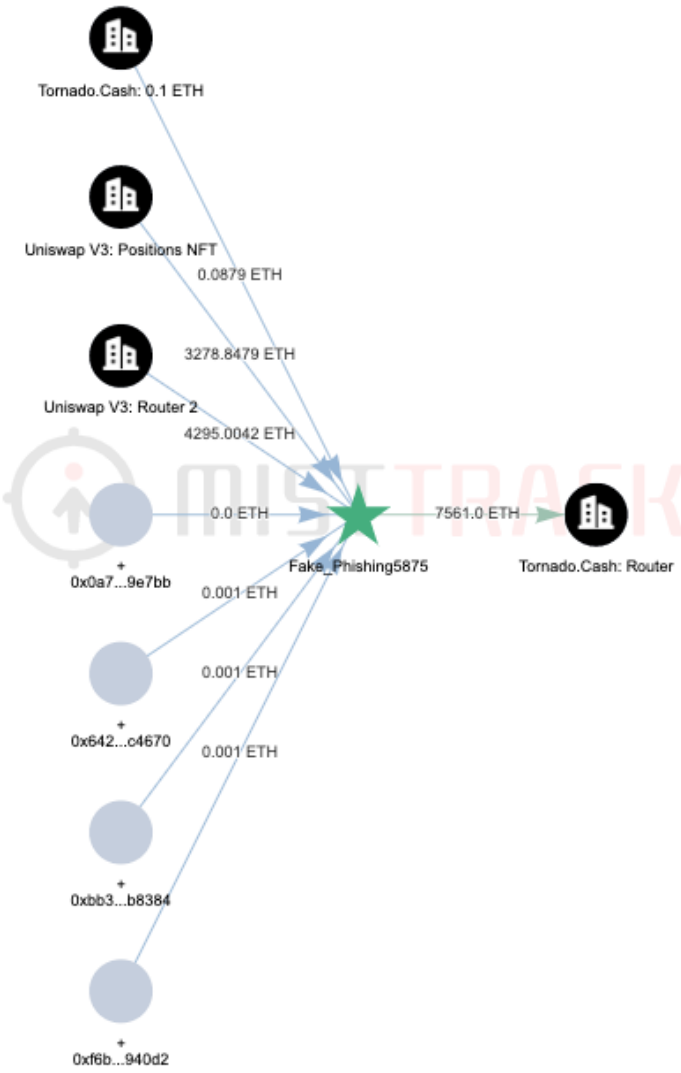
Flow of Transfers:



(Uniswap Phishing Hacker - Timeline of Fund Transfers)

ETH Transfer

While trying to launder the stolen funds, the hacker exchanged 240.42 WBTC for 4,295.0041 ETH through Uniswap. Making the total funds laundered 7,573.8518 ETH.



(Uniswap Phishing Hacker ETH - Diagram of Funds Transferred)

ETH Transfer Chart：

Transfer Method	Funds Transferred
Tornado.Cash	7,561 ETH
Balance	9.46 ETH

3.3.7 ApeCoin Flashloan Arbitrage

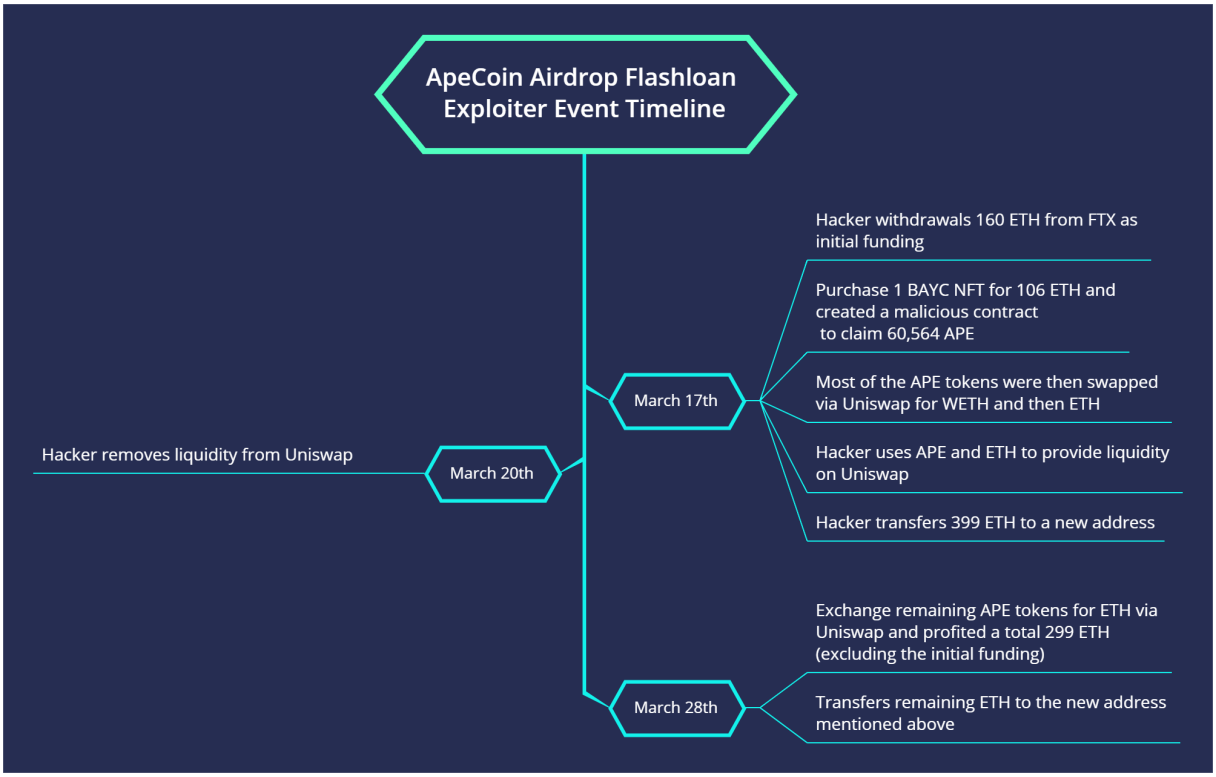
Hackers Address: 0x6703741e913a30d6604481472b6d81f3da45e6e8 (ETH)

Date: 03/17/2022

Amount: 60,564 APE

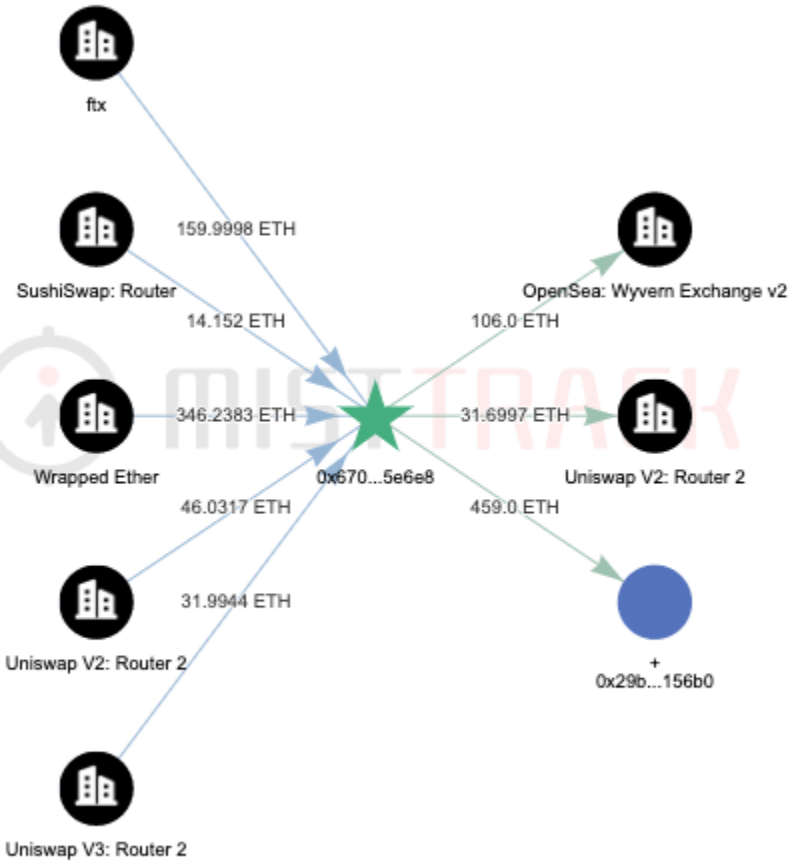
Initial Funding: FTX

Events:



(ApeCoin Airdrop Flashloan Exploiter - Timeline of Fund Transfers)

ETH Transfer



(ApeCoin Airdrop Flashloan Exploiter ETH - Diagram of Funds Transferred)

ETH Transfer Charts:

Transfer Method	Funds Transferred
Balance	459 ETH

Note: The transfer funds include the remaining funds of the attack fee.

3.3.8 BAYC Official Discord Hack

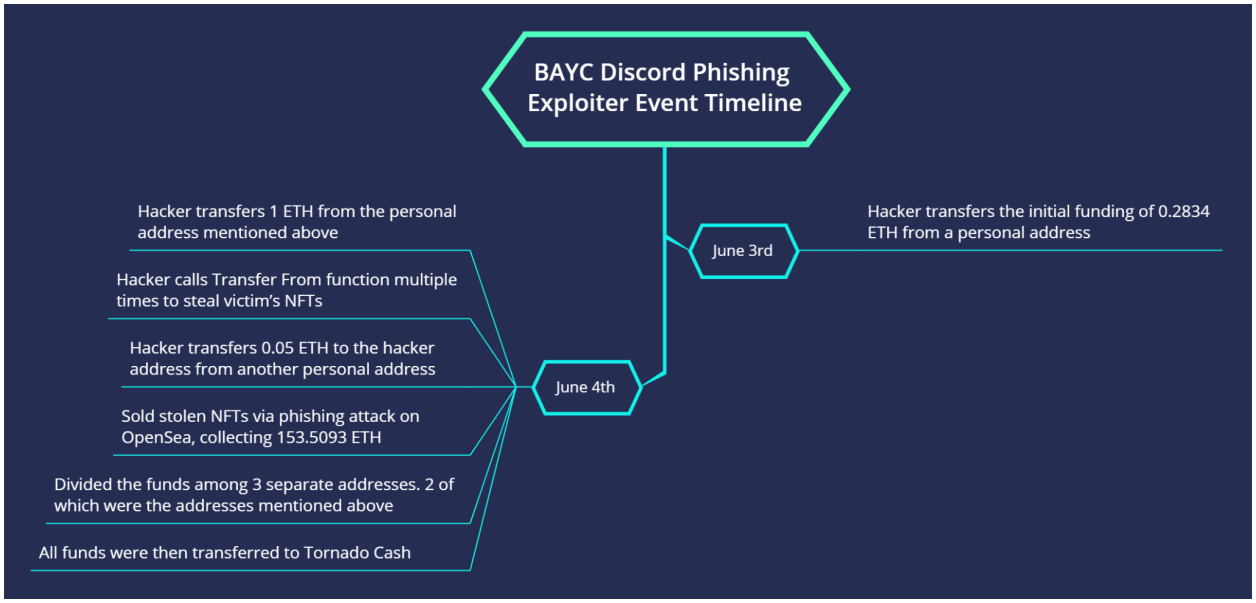
Hackers Address: 0x1079061d37f7f3fd3295e4aad02ece4a3f20de2d (ETH)

Date: 06/04/2022

Amount: NFTs worth over 145 ETH ($256,000)

Initial Funding: transferred personal addresses

Event:



(BAYC Discord Phishing Exploiter - Timeline of Fund Transfers)

ETH Transfer

ETH Transfers Chart:

Transfer Method	Funds Transferred
Tornado.Cash	153 ETH

3.3.9 FEGToken

This section refers to the attack on May 15 as Hacker 1, and attacked on May 16 as Hacker 2.

Hackers Address:

0x73b359d5da488eb2e97990619976f2f004e9ff7c (Hacker 1, ETH/BSC network)

0xf99e5f80486426e7d3e3921269ffee9c2da258e2 (Hacker 2, ETH/BSC network)

Date: 05/15/2022, 05/15/2022

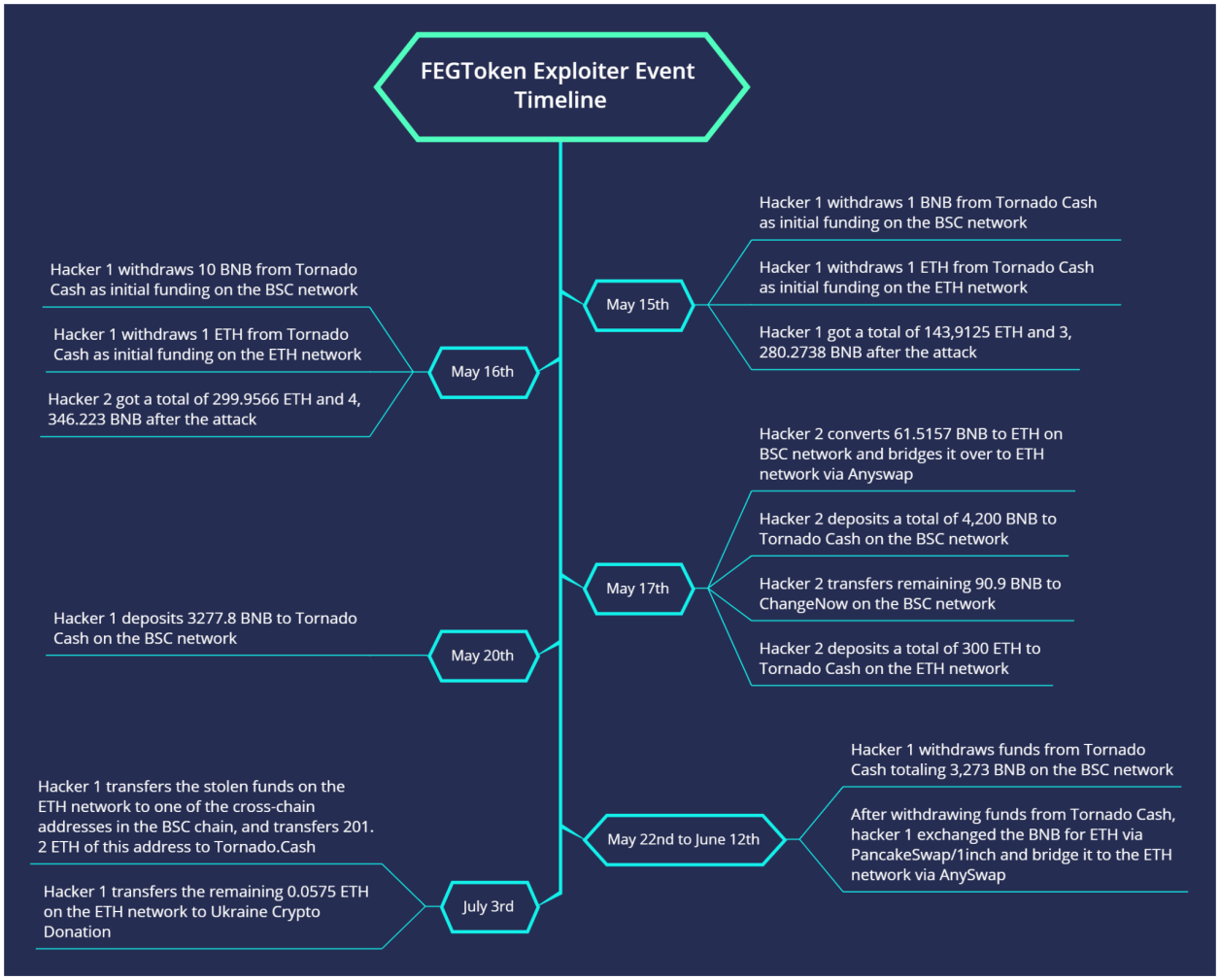
Amount:

Hacker 1: (ETH) 143.9125 ETH, (BSC) 3,280.2738 BNB

Hacker 2: (ETH) 299.9566 ETH, (BSC) 4,346.223 BNB

Initial Funding: Tornado.Cash

Event:



(FEGToken Exploiter- Timeline of Fund Transfers)

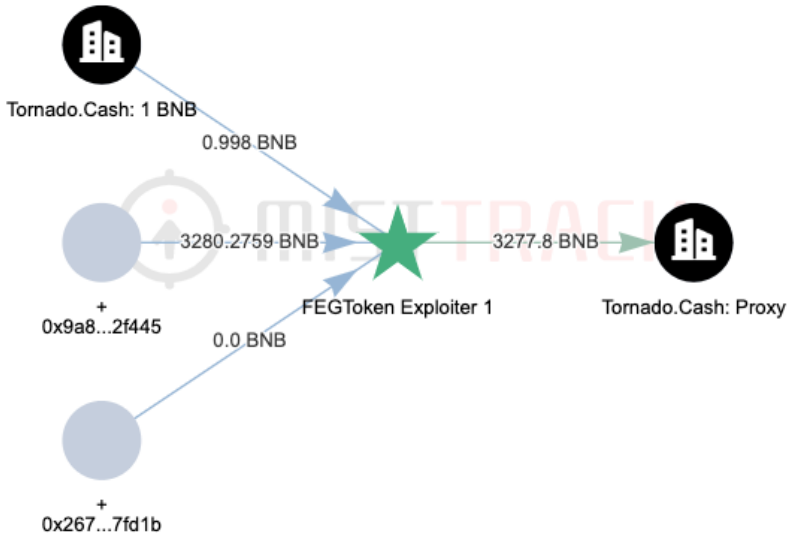
Analysis of the two incidents

Based on blockchain analytics:

- The two hackers used different methods to attack
    - Hacker 1 repeatedly invokes the attack contract
    - Hacker 2 made a single call to attach the contract
- The two hackers also used different techniques to launder the funds
    - Hacker 1 transferred all stolen funds to Tornado Cash

    - Hacker 2 transferred majority of funds to Tornado Cash and the remaining funds to ChangeNOW
- There was also a clear difference between the time these events took place
    - Hacker 1 attacked the protocol on May 15th and laundered the funds on May 20th (BSC) and July 3rd (ETH)
    - Hacker 2 attacked the protocol on May 16 and laundered the funds on the same day

Hacker 1 Transfer of Funds



(FEGToken Exploiter 1 BSC - Diagram of Funds Transferred)

(FEGToken Exploiter 1 ETH - Diagram of Funds Transferred)

Token Transfer Chart：

Network	Transfer Method	Funds Transferred
BSC	Tornado.Cash	3,277.8 BNB
ETH	Tornado.Cash	144.8 ETH

Hacker 1 Transfers on the BSC

On the BSC, a total of 3,277.8 BNB was transferred to Tornado Cash. Based on our analysis, the following withdrawals met the characteristics of the FEGToken exploiter:

- Transactions of 25 or 50 BNB were exchanged for ETH on the BSC via PancakeSwap/1inch, before finally being swapped to Ethereum through AnySwap.
- A transfer to Ethereum was then paused for a while.

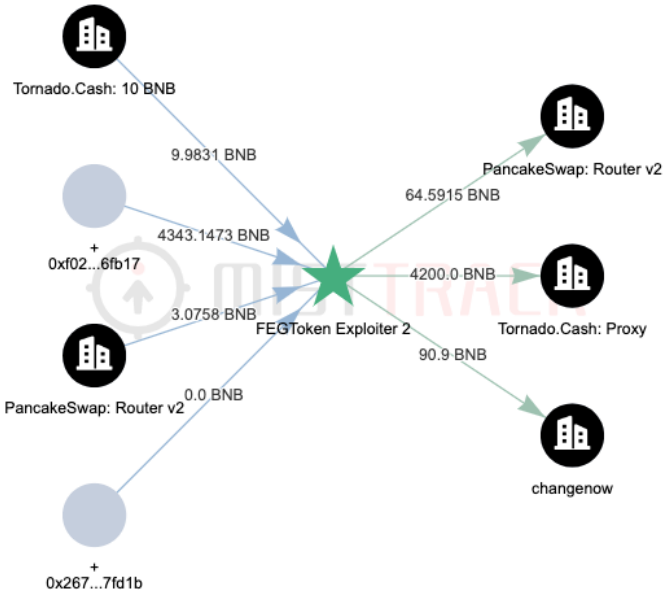
Based on the aforementioned transfer characteristics, a total of 3,273 BNB withdrawals by hackers was identified.

The following is the transfer of funds from Tornado Cash on the BSC:

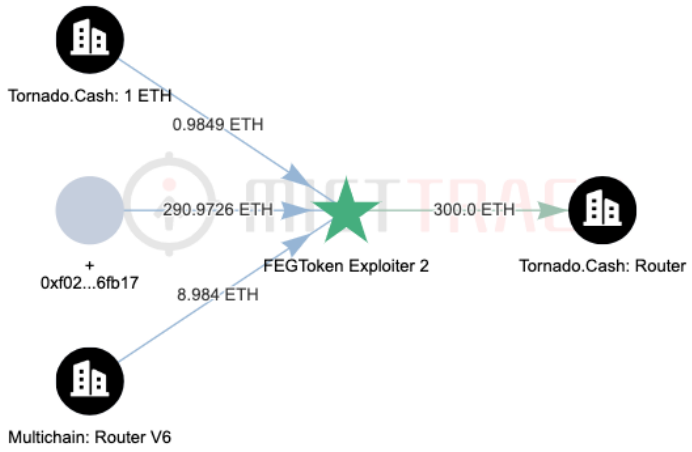
Transfer Method	Funds Transferred
Tornado.Cash	56.5 ETH
Balance	476.9591 ETH

Note: The funds on the BSC have been converted into ETH on the ETH network via AnySwap.

Hacker 2 Transfers



(FEGToken Exploiter 2 BSC - Diagram of Funds Transferred)



(FEGToken Exploiter 2 ETH - Diagram of Funds Transferred)

Token Transfer Chart:

Network	Transfer Method	Funds Transferred
BSC	Tornado.Cash	4,200 BNB
BSC	ChangeNOW	90.9 BNB
ETH	Tornado.Cash	300 ETH

3.3.10 Optimism

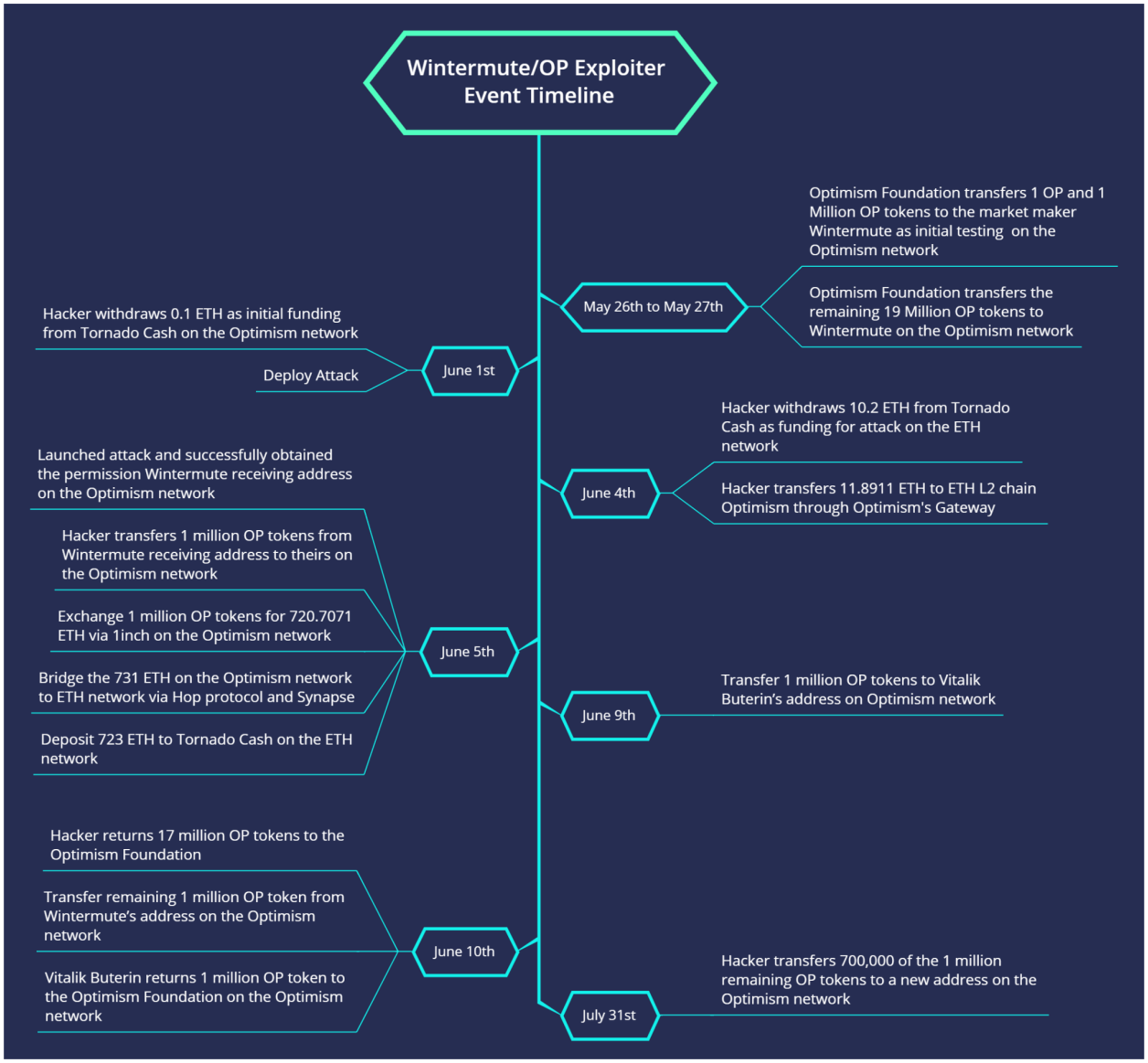
Hacker Address: 0x60B28637879B5a09D21B68040020FFbf7dbA5107 (Optimism)

Date: 06/05/2022

Amount: 20,000,000 OP Tokens

Initial Funding: Tornado.Cash

Events:



(Wintermute/OP Exploiter - Timeline of Fund Transfers)

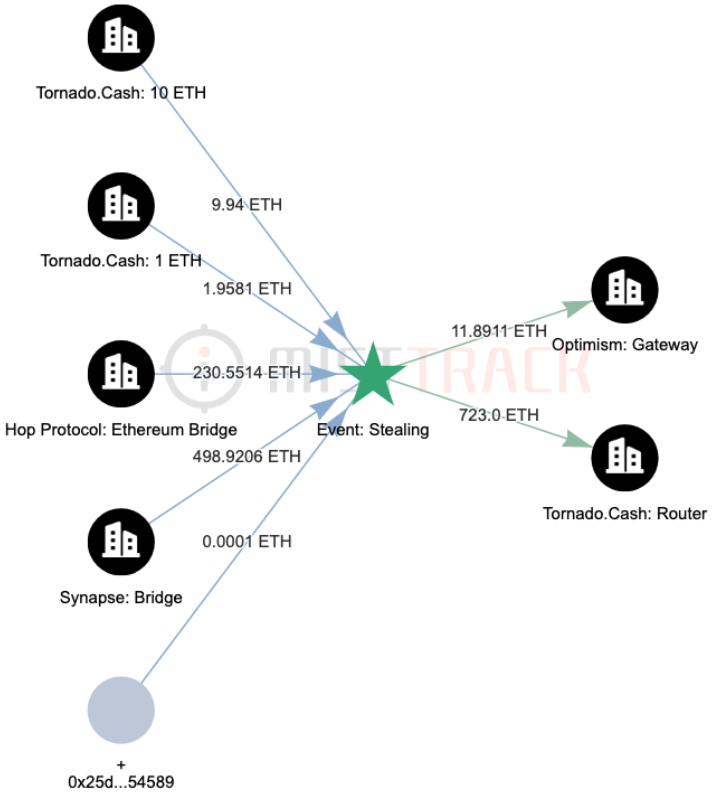
OP Transfer

OP Transfer Chart:

Transfer Method	Funds Transferred
Return to Optimism Foundation	17,000,000 OP
Vitalik Buterin (later returned to Optimism Foundation)	1,000,000 OP

Bridge to ETH network via Hop Protocol and Synapse	1,000,000 OP
Balance	1,000,000 OP

ETH Transfer Flow Chart



(Wintermute/OP Exploiter ETH - Diagram of Funds Transferred)

ETH Transfer Chart:

Transfer Method	Funds Transferred
Tornado.Cash	723 ETH
Balance	5.8744 ETH

Note: This includes the initial funding used for this attack.

3.3.11 MM.finance

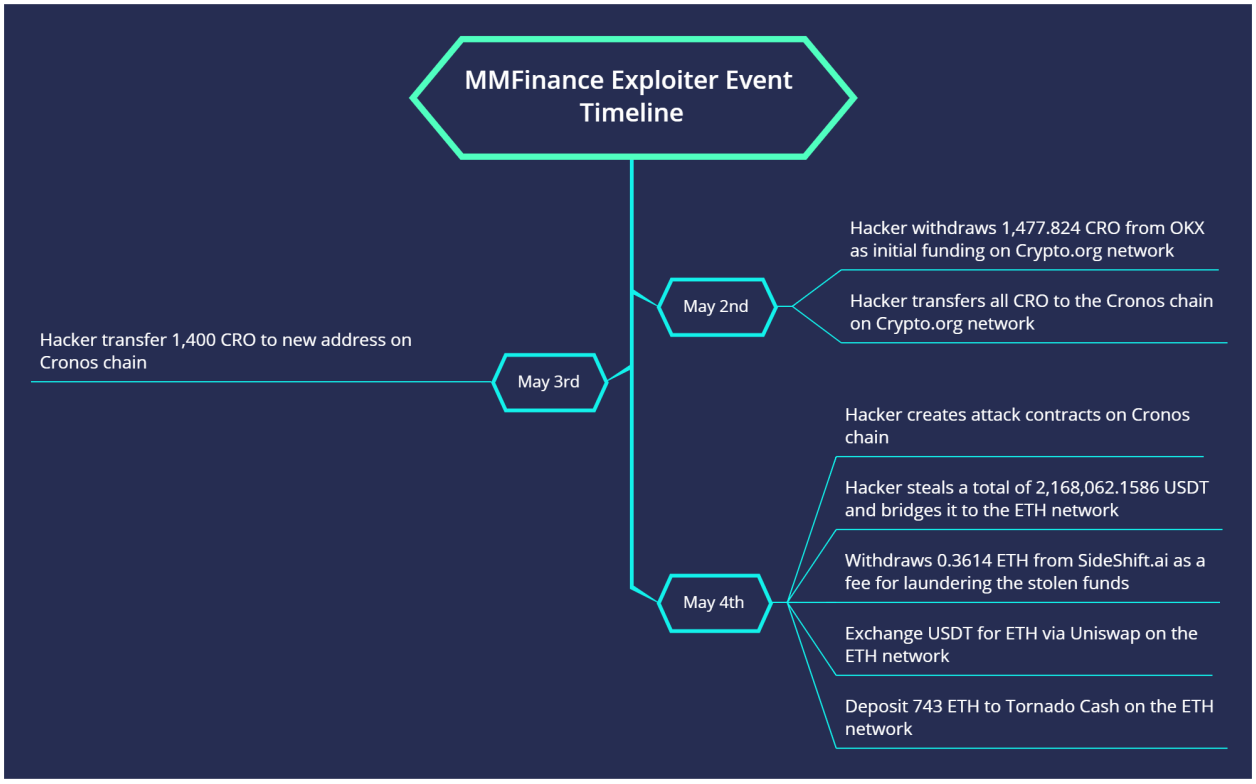
Hackers Address: 0xb3065fe2125c413e973829108f23e872e1db9a6b (Cronos)

Date: 05/04/2022

Amount: $2,000,000

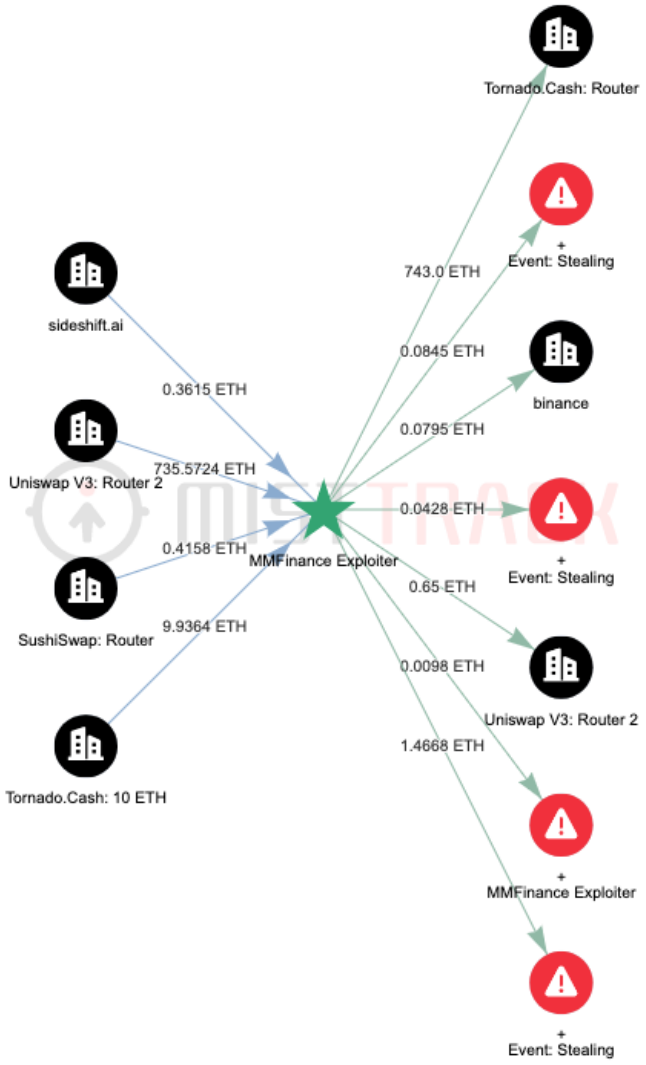
Initial Funding: OKX

Events:



(MMFinance Exploiter - Timeline of Fund Transfers)

ETH Transfer



(MMFinance Exploiter ETH - Diagram of Funds Transferred)

ETH Transfer Chart:

Transfer Method	Funds Transferred
Tornado.Cash	743 ETH

4. Summary

This report analyzes the first half of 2022 in terms of blockchain security incidents and anti-money laundering activities. In general, it can be divided into the following two points:

Increase in Blockchain-related incidents and methods used

According to statistics, there were 187 security incidents in the first half of 2022, with losses near $1.976 billion. DeFi security incidents accounted for 53% (about 100 incidents), and it seems to have become more appealing for hackers to partake in. Among these, popular projects involving the most damage were concentrated around cross-chain protocols. Since cross-chain projects are highly funded and centralized, it has become the target of many sophisticated attacks. In the first half of the year, 75% of these incidents with losses over hundreds of millions were cross-chain related, namely Ronin Network, Wormhole, and Harmony.

The majority of incidents within the first half of the year can be classified into four categories:

1. Contract Vulnerabilities
2. Scams including Rug Pull, phishing attacks, etc.
3. Private key compromises
4. Front-end malicious attacks

With the rapid growth of Web3, phishing attacks against NFTs are becoming increasingly sophisticated, with a particular emphasis on the spread of phishing links following the compromise of media platforms like Discord and Twitter. We advise that everyone proceeds with caution.

Analysis of AML & Blockchain Related Incidents

This report discusses various security incidents that resulted in major losses as well as common incidents and the extent of their influence. In addition to discussing new methods used by malicious actors, it also includes a brief description of each method and the amount stolen. This

report outlines numerous security incidents that resulted in significant losses, as well as common incidents and their impacts to the crypto ecosystem. In addition, it also discusses new methods employed by malicious actors, a brief description of the methods involved, and the amounts that were stolen.

MistTrack was used to perform an anti-money laundering analysis on eleven security incidents. The answers to our questions regarding initial funding for attacks and where the funds were sent were revealed through the use of our analysis techniques. We also developed an algorithm using blockchain analytics to evaluate withdrawals from Tornado Cash and ChipMixer.

During our investigation, we discovered that the majority of the incidents were on the Ethereum and Bitcoin networks. 74.6% of stolen funds on the Ethereum network were transferred to Tornado Cash, while 48.9 % of stolen funds on the Bitcoin network were transferred to ChipMixer to avoid detection.

Bitcoin is frequently the preferred cryptocurrency for major security incidents and crypto laundering activities that involve The Lazarus Group. Bitcoin provides more anonymity and flexibility in mixing methods than Ethereum. Additionally, the Lazarus Group has more experience with laundering bitcoin, making them more adept at the process.

5. Disclaimer

The data contained in this report was compiled using information from our anti-money-laundering (AML) platform, MistTrack, as well as our expertise of the blockchain industry and using the SlowMist Hacked database of blockchain-related incidents. Due to the "anonymous" nature of the blockchain, we cannot guarantee the absolute accuracy of all the data in this report, nor are we liable for any errors, omissions, or losses resulting from its use. This report does not serve as the basis for any investment recommendations or analysis.

We appreciate your feedback and apologize for any errors that may have been overlooked.

6. 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

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 Products

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 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 Public Account

7. Media Partners

SLOWMIST

Focusing on Blockchain Ecosystem Security