BEOSIN
Blockchain Security

Footprint
Analytics

BEOSIN 2022 Q2 WEB3 SECURITY REPORT

SECURING WEB3.0
BLOCKCHAIN ECOSYSTEM

CONTENTS

Data source:
https://www.footprint.network/@Beosin/Footprint-Beosin-Q2-Report

2022 Q2 Web3 Security Overview

A total of 48 major exploits were monitored, with a total loss of approximately $718.34 million

In the second quarter of 2022, 48 major attacks were monitored in the Web3 space, with total losses of approximately $718.34 million, down approximately 40 percent from $1.2 billion in the first quarter and approximately 2.42 times the losses in Q1 2021 ($296.56 million).

From January to June 2022, assets lost in the Web3 space due to attacks totaled $1,912.87 million.

Q Over Q Growths

Date	Total Loss
2022-Q1	1,194,525,820
2022-Q2	718,343,550
Quarter-over-quarter	-0.3986

Q on Q Growths

Date	Total Loss
2021-Q2	296,560,000
2022-Q2	718,343,550
Quarter-on-Quarter	1.42

April was the most active month for hacking. May saw a significant decrease in the number of attacks and losses; hacking activity increased in June.

All chains and attacked projects saw a significant decrease in TVL values in May. Most projects experienced a decrease in TVL immediately after they were attacked.

The most common hacking techniques continue to be contract vulnerability exploitation and flash loans. Approximately 45.8% of attacks were contract exploits. The greatest losses were caused by flash loans, totaling $233 million.

Only 52% of the attacked projects were audited.

By project type, DeFi continues to have the greatest rekt frequency; approximately 79.2% of attacks occur in the DeFi domain.

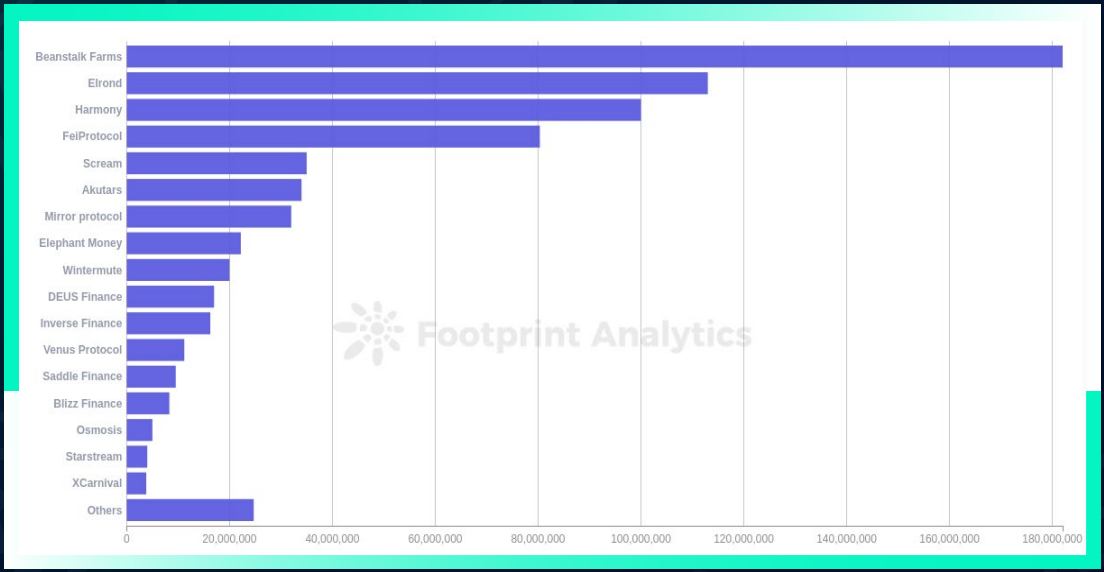
By chain, the greatest loss this quarter was on Ethereum, $381.35 million. The most frequently attacked chain was BNB Chain, with 26 exploits.

Approximately $418.89 million in stolen funds were transferred to Tornado.cash by hackers, representing 58.3% of the total amount stolen during the quarter.

Forty-three major rug pull incidents on the chain were monitored this quarter, with total losses of approximately $34,266,402. From incomplete statistics, Discord servers were hacked more than 151 times. Rug pull and phishing security incidents were frequent in May and June.

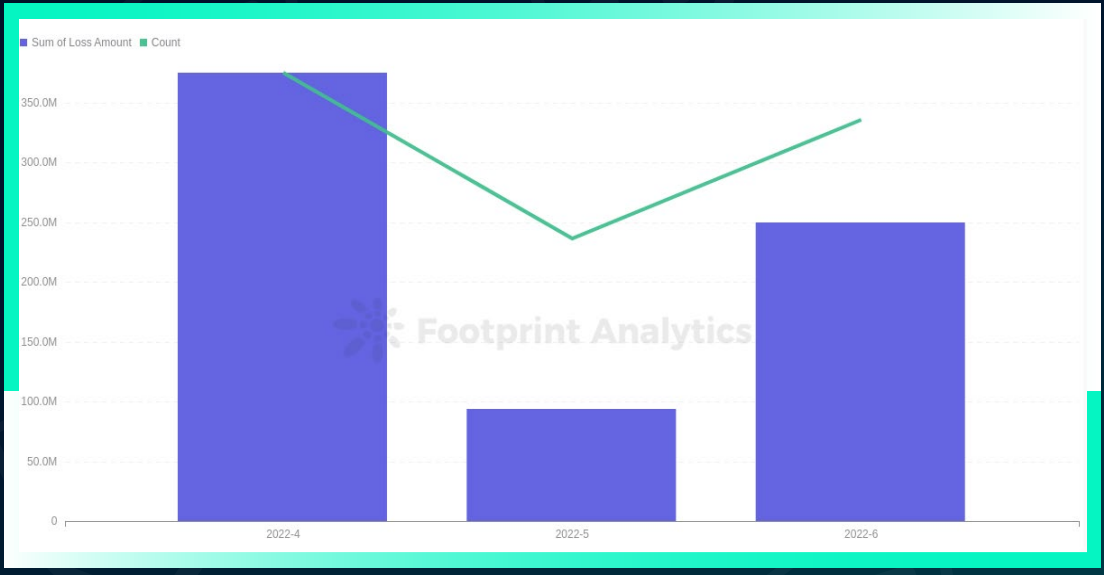
Overview of exploits

April was the most active month for exploits in Q2



In Q2 2022, 48 major attacks were monitored in the Web3 space, with a total loss of approximately $718.34 million. There were three attacks with losses of $100 million or more, 12 attacks with losses of $10 million or more, and 28 attacks with losses of $1 million or more. The three greatest losses were from Beanstalk Farms, Elrond, and Harmony, with $182 million, $113 million, and $100 million, respectively.

April 2022 was the most active month for hacking in the quarter, with 19 major security incidents and losses of approximately $374,889. May saw a significant decrease in the number of attacks and total losses, perhaps related to significant shrinkage in cryptocurrency market cap in May. June saw a significant increase in hacking frequency and project losses compared to May, although the market did not see an increasing trend.

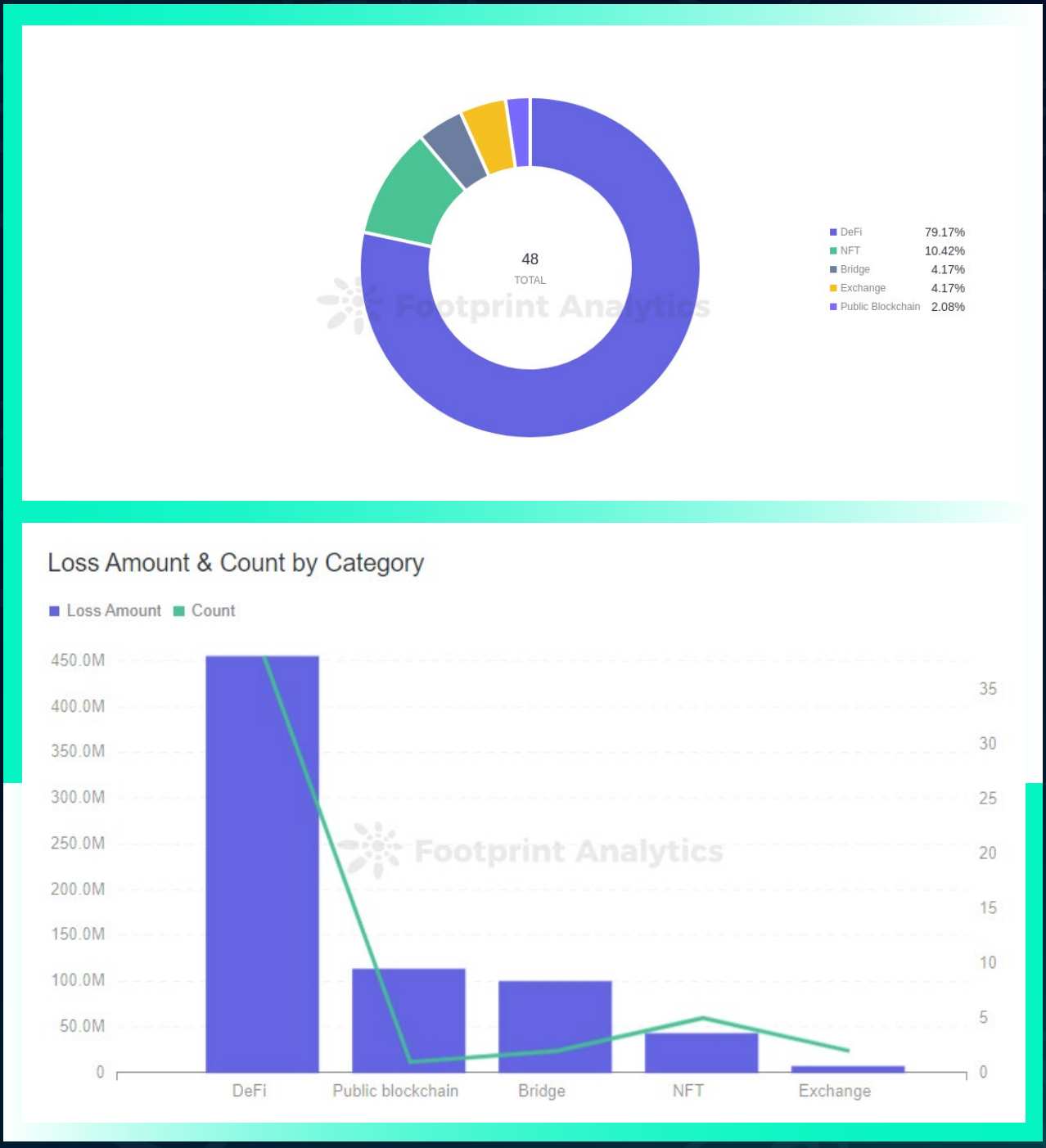


Types of rekt projects

79.2% of exploits occur in the Defi space

As in Q1, DeFi continued to be a major target of hackers, with approximately 79.2% of attacks occurring in the Defi space and a total loss of approximately $454.74 million, 63.3% of the total losses in Q2.

Two cross-chain bridge attacks continued to occur this quarter, with cumulative losses of approximately $100 million. In Q1 2022, the total loss from the four cross-chain bridge attacks was $950 million, bringing the loss from cross-chain bridge attacks to $1.05 billion in the first half of 2022.



TVL analysis of attacked projects

TVL of some projects decreased to zero after being attacked

Almost all attacked projects experienced a decrease in TVL in May, most with an immediate decrease in TVL after they were attacked. For some projects, including Beanstalk and Blizz Finance, TVL immediately decreased to zero after the attack.

In most cases, the loss in TVL after an attack was less than 30%. Blizz Finance and Beanstalk experienced TVL losses of 100% and 500%, respectively.

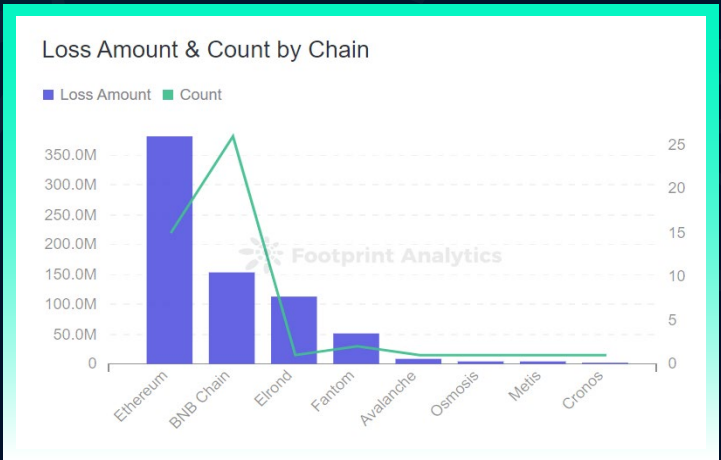
Date	Protocol Slug	TVL	Loss Amount	Pct
2022-4-2	inverse-finance	67,344,176	15,000,000	22.27%
2022-4-8	starstream	28,662,864	4,000,000	13.96%
2022-4-17	beanstalk	35,934,428	182,000,000	506.48%
2022-4-28	deus-finance	60,549,740.02	17,000,000	28.08%
2022-4-30	fei-protocol	352,825,568	80,340,000	22.77%
2022-4-30	saddle-finance	278,756,557.24	9,540,000	3.422%
2022-5-4	mm-finance	745,404,608	2,000,000	0.2683%
2022-5-13	blizz-finance	8,284,470.5	8,300,000	100.19%
2022-5-13	venus	1,012,455,104	11,200,000	1.106%
2022-5-16	scream	98,347,120	35,000,000	35.59%
2022-6-8	apollox	13,024,072	1,600,000	12.28%
2022-6-8	osmosis	220,895,040	5,000,000	2.264%
2022-6-16	inverse-finance	13,258,454	1,260,000	9.503%

Loss amount by chain

Ethereum saw the greatest loss; BNB Chain saw the most attacks

Ethereum lost the most assets this quarter, $381.35 million. BNB Chain was the most frequently attacked chain, with 26 exploits.

Chains with attacks in two consecutive quarters include Ethereum, BNB Chain, Fantom, and Cronos. Solana lost $374 million in the first quarter from two exploits but did not experience any major security incidents this quarter.



In the second quarter, all chains saw a significant decrease in TVL in May. Ethereum and BNB Chain, with the top two TVL, continued to be the main targets of hackers. A total of $718.34 million was lost in attacks in the second quarter, more than the total combined TVL of Osmosis, Elrond, and Metis in June.

Chain	Sum of Loss Amount	Avg TVL	Pct
Metis	4,000,000	123,950,280.75	3.227%
Fantom	52,000,000	5,824,023,179.65	0.8929%
BSC	49,539,085	10,551,478,231.19	0.4695%
Ethereum	340,900,000	98,980,928,368.9	0.3444%
Avalanche	8,300,000	6,945,411,851.15	0.1195%

Chain	Attacked Count	Q2 Total Protocal Count	Pct
BSC	23	324	7.099%
Metis	1	21	4.762%
Ethereum	11	428	2.57%
Fantom	2	211	0.9479%
Avalanche	1	181	0.5525%

In terms of DeFi projects, the largest loss amount of DeFi projects was on Ethereum, but the percentage of the average TVL in Q2 was not high; Metis lost the highest percentage of TVL instead. The smallest percentage is Avalanche.

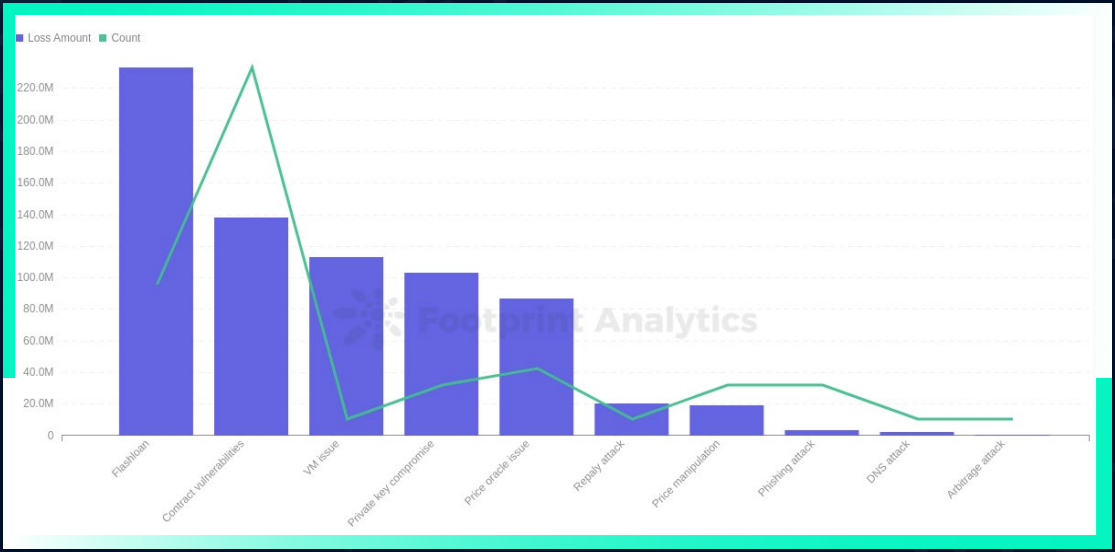
In terms of the number of attacks on DeFi protocols, BNB Chain had the highest proportion of attacked DeFi protocols to its total number of protocols in Q2, reaching 7%. The DeFi ecosystem on Metis is not yet rich enough, and although there was only one attack, it accounted for a higher percentage in both loss amount and attacked count.

Analysis of Hacking Techniques

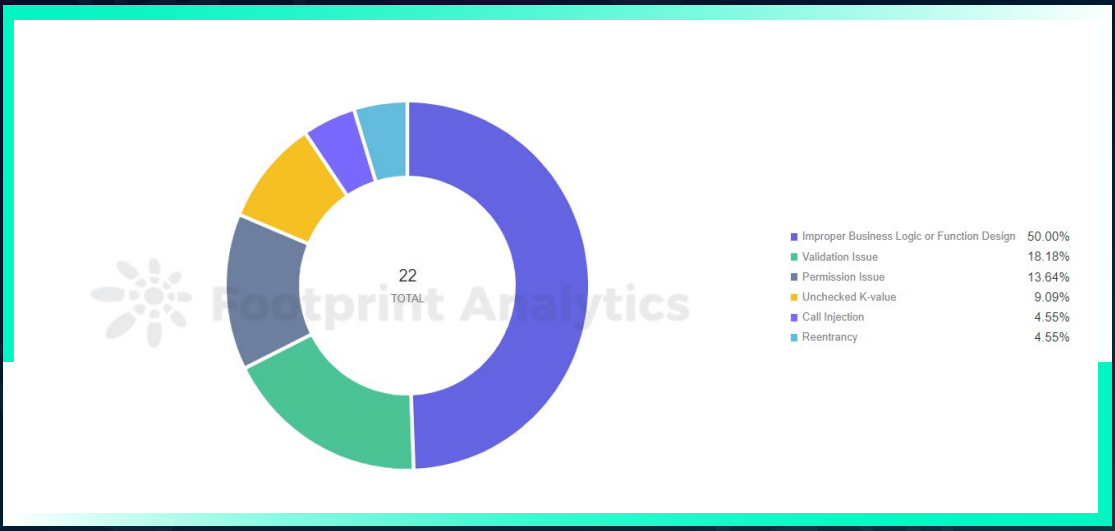
The most common hacking techniques continue to be contract exploits and flash loans

Contract vulnerability exploitation was the most common attack method this quarter, with 22 attacks, accounting for 45.8% of attacks and a total loss of approximately $138 million. Flash loans were the second most common attack method, with nine attacks and losses of $233 million this quarter, the greatest loss from any hacking method.

As in Q1, the most common hacking techniques in the blockchain space continue to be contract exploits and flash loans (50% and 24% of attacks, respectively, in Q1). Losses due to compromised private keys were $131.15 million; private key security continues to be a concern.

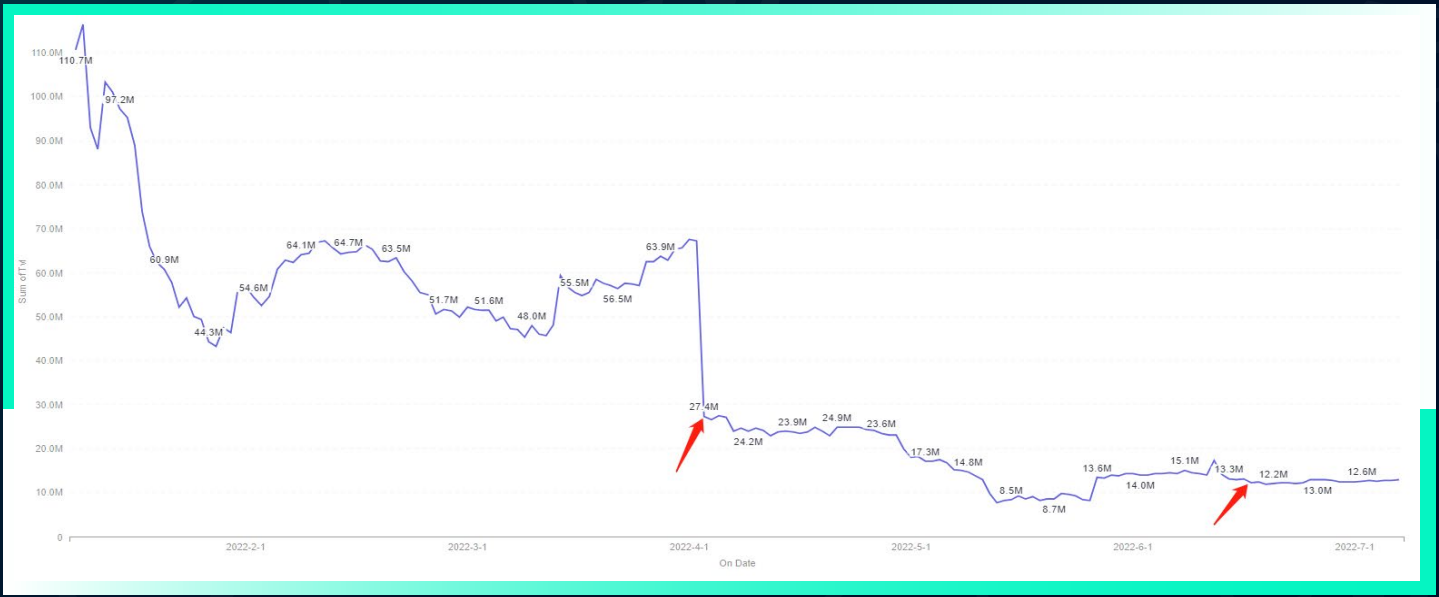


The main vulnerabilities exploited this quarter include improper business logic/function design, validation issues, permission issues, unchecked k-values, reentrancy, and call injection vulnerabilities. The most exploited vulnerability is improper business logic/function design, far ahead of the other vulnerabilities. Reentrancy vulnerability was exploited by hackers only once, producing a loss of $80.34 million.



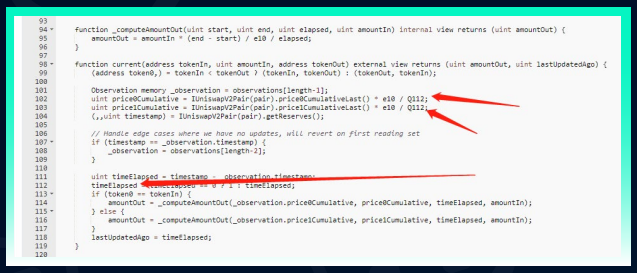
Typical Security Incident Recap

7.1 Inverse Finance attacked twice

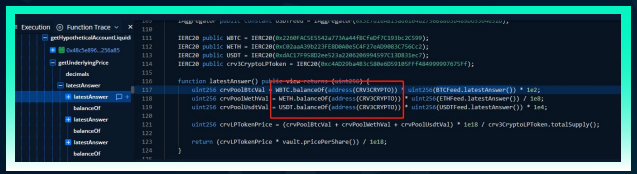


Incident details:

On April 2, 2022, Inverse Finance suffered a price manipulation attack with a loss of approximately $15 million. The main cause of the attack was the short time window used by the TWAP oracle. In calculating the price of the Xinv token, it relies on the pair WETH/INV. As the pair pool had already been manipulated, with the short timeElapsed interval, the attacker was able to manipulate the xINV token price as long as the current block was not called in.



On June 16, 2022, Inverse Finance was hacked again, with a loss of $1.2 million. The main cause was use of the balanceOf function in the project contract in calculating the price of collateral; the attackers were able to increase the price of anYvCrv3Crypto collateral by exchanging large amounts of assets.



Recommendations:

Obtaining token prices should not rely on real-time token balances, instead using a TWAP oracle with an adequate time window.

7.2 Akutars: $34 million locked due to smart-contract vulnerability

Incident details:

On April 24, 2022, $34 million was locked from withdrawals in the Akutars NFT project due to a smart-contract vulnerability. The project contracts were not audited by a security firm. Upon analysis, the Akutars contract was found to contain two vulnerabilities.

Vulnerability I.

The first contract vulnerability was in processRefunds; the designer performs a loop refund based on the refundProgress counter. The call function is used to perform the refund operation, and the refund result is used as the determination condition for the require function. If an attacker in the queue performs a refund operation, and an attacker in the fallback performs a malicious revert, the entire queue behind the attacker cannot be refunded. Fortunately, this vulnerability was not actually exploited.

Vulnerability I.

The second vulnerability caused $34 million in assets to be locked in the contract.

The claimProjectFunds function is mainly used for project withdrawals. In the function require(refundProgress >= totalBids), refundProgress indicates how many user refunds have been processed, and totalBids indicates how many NFTs have been bid by all users. As a user can bid multiple NFTs, refundProgress may be smaller than totalBids.

```
618     function claimProjectFunds() external onlyOwner {
619         require(block.timestamp > expiresAt, "Auction still in progress");
620         require(refundProgress >= totalBids, "Refunds not yet processed");
621         require(akuNFTs.airdropProgress() >= totalBids, "Airdrop not complete");
622
623         (bool sent, ) = project.call{value: address(this).balance}("");
624         require(sent, "Failed to withdraw");
625     }
```

The refund function processRefunds: require(_refundProgress < _bidIndex); bidIndex means that all users are participating in the bidding, and refundProgress will never be higher than bidIndex.

However, the value of bidIndex was 3669 and the value of totalBids was 5495. Thus, the judgment condition that refundProgress>=5495 and refundProgress<3669 did not hold, and the project was unable to perform subsequent withdrawal operations. Here, refundProgress should have been compared with bidIndex; the developer made a low-level mistake, resulting in $34 million in assets on the project side being locked from withdrawal.

Recommendations:

A professional security audit is essential before the project goes live.

7.3 Beanstalk Farms: Hackers obtain $80 Million through malicious proposal

Incident details:

On April 17, 2022, the algorithmic stablecoin project Beanstalk Farms was the victim of a flash-loan attack, with losses of nearly $80 million and the protocol losing $182 million. This project had the greatest loss for the quarter.

The attacker initiated a proposal to withdraw Beanstalk:Beanstalk Protocol funds the day before the attack, and called an emergencyCommit to execute the proposal, as the project owner stipulated that voting could not start until one day after the proposal.

During the attack, the attackers exploited the vulnerability that "the number of votes in the voting contract is calculated from the proposal token holdings of the account" and borrowed over $1 billion via flash loan in exchange for tokens, transferred them into the mining pool, obtained many proposal tokens, and ensured that the proposal could be passed without other votes. The proposal was eventually passed and executed. The attacker successfully withdrew the project funds and repaid the flash loan for a gain of approximately $80 million.

```
balanceOfRoots in GovernanceFacet:34
29          emit Vote(account, bipId, balanceOfRoots(account));
30      }
31
32      function recordVote(address account, uint32 bipId) internal {
33          s.g.voted[bipId][account] = true;
34          s.g.bips[bipId].roots = s.g.bips[bipId].roots.add(balanceOfRoots(account));
35      }
36
```

```
180     function emergencyCommit(uint32 bip) external {
181         require(isNominated(bip), "Governance: Not nominated.");
182         require(
183             block.timestamp >= timestamp(bip).add(C.getGovernanceEmergencyPeriod()),
184             "Governance: Too early.");
185         require(isActive(bip), "Governance: Ended.");
186         require(
187             bipVotePercent(bip).greaterThanOrEqualTo(C.getGovernanceEmergencyThreshold()),
188             "Governance: Must have super majority."
189         );
190         _execute(msg.sender, bip, false, true);
191     }
```

Recommendations:

1.The funds used for voting should be locked in the contract for a certain period of time to avoid use of the current fund balance of the account to count the number of votes.

2. Projects and communities should monitor all proposals; if a proposal is malicious, timely measures should be taken during the proposal voting period to discard the proposal, preventing voting and implementation.

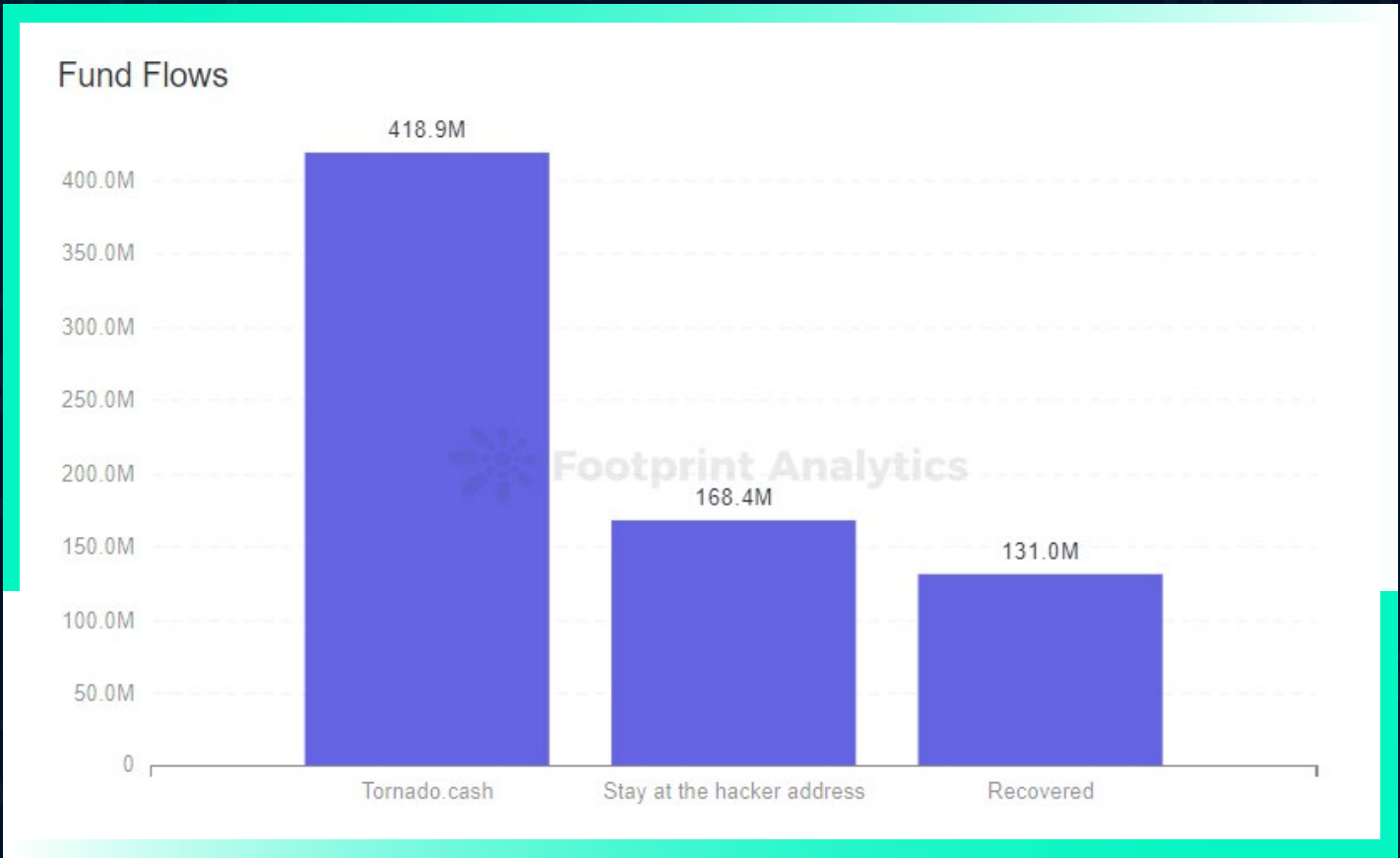
3. Consider prohibiting contract addresses from participating in voting.

Fund Flow Analysis

Approximately $418.89 million in stolen funds were transferred into Tornado.cash

Approximately $418.89 million in stolen funds were transferred to Tornado.cash by hackers in the second quarter of 2022, representing 58.3% of the total stolen during the quarter; $131 million in assets were recovered and $168.45 million in assets remained at the hacker's address without coin mixing or transfer to exchanges.

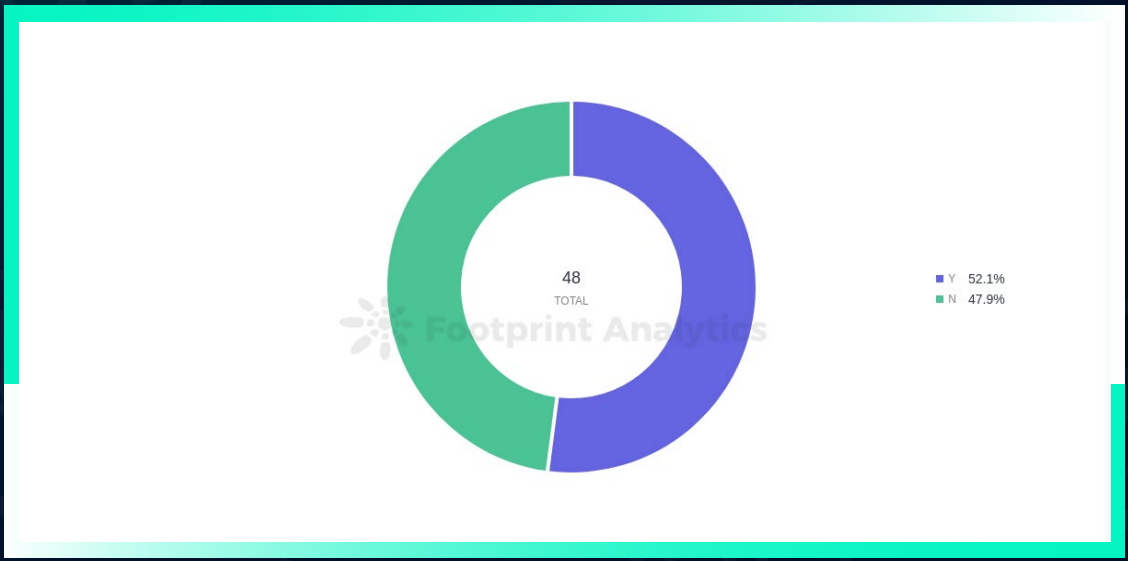
The data show that Tornado.cash continues to be commonly used by hackers to launder money. Recovery of funds was better in this quarter than in the previous quarter. In some cases, project owners and hackers negotiated through on-chain messages, with some hackers opting to return some of the stolen funds to "avoid legal sanctions".



Project Audit Analysis

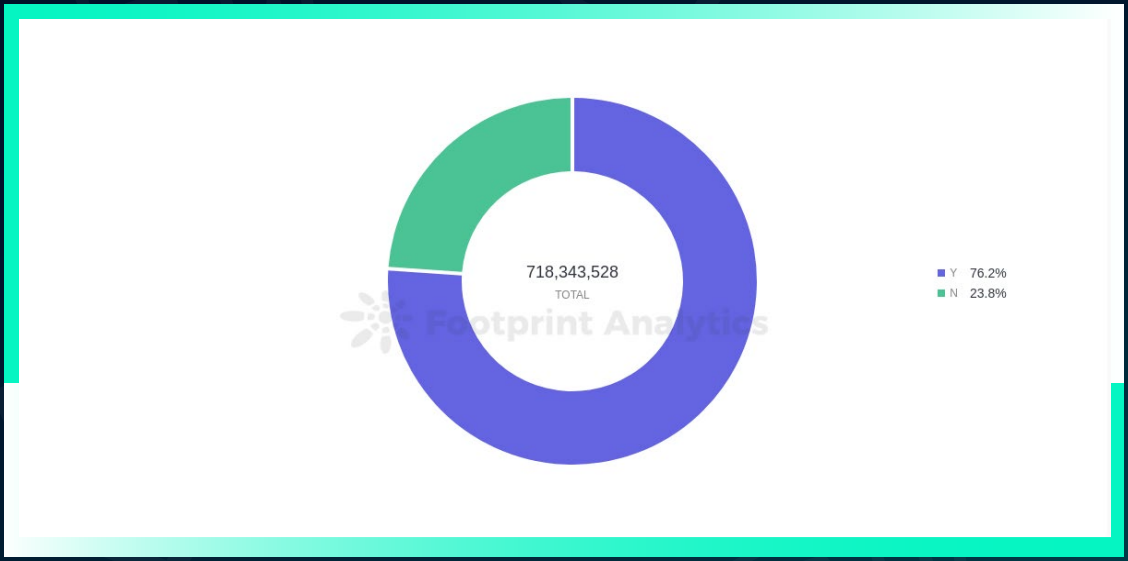
Only 52% of projects were audited

Only 52% of attacked projects were audited, compared to 70% in the previous quarter. Projects audited in this quarter lost a total of $547.63 million, 76.2% of the total lost, much more than in the previous quarter.



Although losses from audited projects totaled $547.63 million, this does not mean that audits are no longer effective.

As more security companies enter the audit business, the audit market is quite mixed. Some auditing companies are questionable. Vulnerabilities in smart contracts that should have been audited were not identified. Project devs and investors began to question the validity of the audits. The most common vulnerability in this quarter is "improperly designed business logic/functions", which can be discovered during the audit phase. Thus, it is recommended that project parties find a reputable security company to conduct an audit before the project goes live.

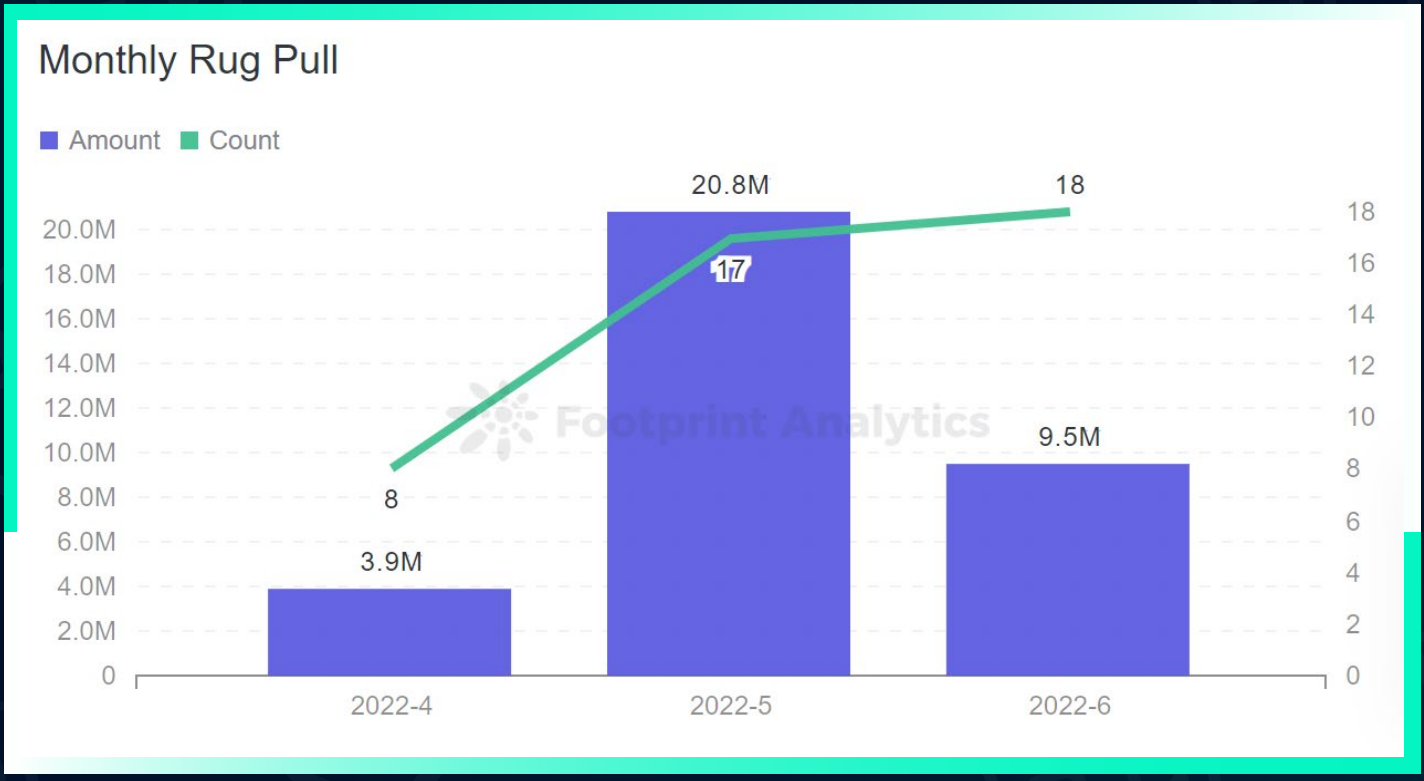


Rug Pull Analysis

$34,266,402 was lost in rug pulls

A rug pull usually refers to withdrawal of devs from the DEX liquidity pool or sudden abandonment of a project, absconding with investor funds without any indication. In the second quarter of 2022, 43 major on-chain rug pulls were monitored, with total losses of approximately $34,266,402.

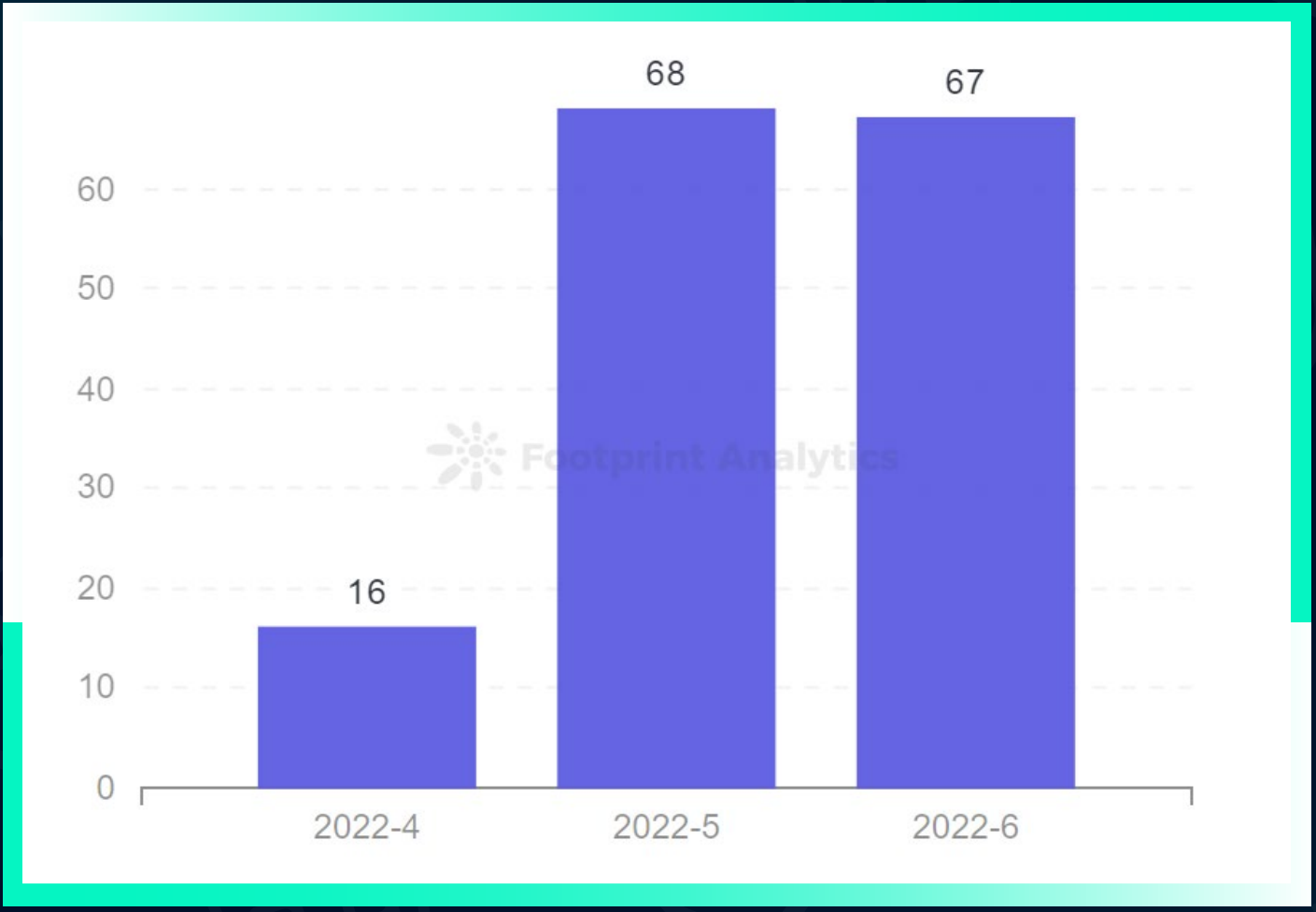
The exploit data show that hacker activity decreased significantly in May, although rug pulls occurred most frequently in May. With the TVL of some public blockchains and projects decreasing significantly in May, some projects chose to rug pull, resulting in losses to a large number of investors. It may have been that these projects could not continue, or it was thought that a rug pull was better than waiting for the TVL to drop to zero, or a rug pull was already planned, with a sharp decrease in TVL accelerating the process.



Discord Phishing Analysis

Discord phishing cases were frequent this quarter

From incomplete statistics, more than 151 Discord servers in the Web3 domain, including Opensea, BAYC, Moonbirds, RTFKT, Akutars, Doodles, and Otherside were compromised in Q2 2022; May and June were particularly active. Some servers were attacked twice or three times during the quarter.



Similar to rug pulls, phishing security incidents can increase with a downturn in the crypto market. Discord phishing methods were observed this quarter in a variety of forms, including compromised bot accounts, phishing links sent by DMs from fake admins or bots, and fake Discord invitation links spread through social media. Users and projects should heighten anti-phishing awareness and protect their assets, especially in more bearish markets.

Summary

DeFi security remained a focus of concern in Q2 2022, with approximately 79.2% of attacks occurring in the Defi space. For two consecutive quarters, DeFi has been the focus of hacker attacks. Although NFT, cross-chain bridges, and exchange security incidents are not as frequent as DeFi incidents, several incidents involved large losses. Web3 projects of all types should strengthen security.

Approximately 45.8% of attacks this quarter were contract vulnerability exploits, the vast majority of which could have been prevented during the audit phase. However, only 52% of rekt projects were audited this quarter. It is recommended that projects seek a reputable auditing company to conduct an audit before going live.

During the quarter, approximately $418.89 million in stolen funds were transferred by hackers to Tornado.-cash for money laundering. Approximately $131 million in assets were recovered; most recovery was the result of negotiating with hackers on-chain to voluntarily return some of the stolen funds. The problem of stolen funds entering Tornado.cash can be solved. Beosin has been successful in tracing stolen funds, including funds entering Tornado.cash. It is suggested that when a project encounters a hack, it enlists a security company for funds tracing, in addition to negotiating with the hacker to return funds.

TVL values for all public blockchains and projects have fluctuated greatly this quarter. There have been cases of abnormal project funding and risky transactions caused by security incidents. It is recommended that project owners and investors monitor project operations. Beosin EagleEye can comprehensively monitor project operations, assess potential project risks, monitor fund flows of target addresses in real time, and provide timely warnings for threat intelligence.

In this quarter of market downturn, rug pulls, phishing, and other security incidents were more frequent; some Web2 attack methods are still active in the Web3 world. All projects and users should heighten security awareness, protect private keys, avoid clicking on links from unknown sources, and verify all information through multiple channels. Adding an anti-phishing extension can also help identify potentially malicious websites.

Link to extensions:

https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=en

Special thanks to Footprint Analytics for supporting this report with charts and data. All charts and graphs in this report can be viewed online at https://www.footprint.network/@Beosin/Footprint-Beosin-Q2-Report.

About Beosin

Beosin is a leading global Web 3.0 blockchain security company co-founded by several professors from world-renowned universities. We provide integrated blockchain security services and products to serve 1 million+ users in the global blockchain ecosystem.

Blockchain Security Audit Service

Include smart contract and blockchain platform audit to verify and identify any vulnerabilities in the code and provide detailed audit reports with improvement recommendations.

Beosin Alert Service

Provide real-time alerts by conducting comprehensive analysis of transaction risks, large outflows, flash-loans, ownership transfer, price drop and other types of threats.

Cryptocurrency Tracing Service

Provide one-stop on-chain transaction and asset flow analysis with detailed investigation covering transaction behavior analysis, asset flow tracing, address monitoring, forensics reports, etc.

Provide formal verification, static scanning and fuzzy testing to assess smart contract security. It can automatically detect vulnerabilities and precisely identify risky codes.

Identify suspicious transactions and risks, and provide workable recommendations by automatically assessing contract security status and monitoring real-time on-chain operations.

Provide capabilities to trace stolen assets and mixed coins; assess wallet addresses and transactions security; and monitor suspicious wallet addresses. The product can be used for performing KYT and AML compliance assessments.

Contact @ beosin.com
www.beosin.com
t.me/beosin
twitter.com/BeosinAlert
twitter.com/Beosin_com
discord.com/invite/B4QJxhStV4

About Footprint Analytics

Footprint Analytics is a one-stop on-chain data analytics platform that currently covers 17 chains along with 900+ DeFi protocols, 20000+ NFT collections, 1600+ GameFi projects and over 100,000 token prices and more.

Our services and expertise

Research Service and Tool

Weekly & monthly reports
Indicator alerts
Custom and on-demand research

Data API

A unified API allows you to pull detailed, historical and granular blockchain data

Footprint Analytics Widget

Show blockchain data on your site
Supports multiple templates
Supports custom configurations

Marketing Tool

Competitive analysis and tracking
Find and incentivize target users and track conversion
Discover user portrait

Social Media Sharing Tool

Build and share your profile
Whitelabel your charts and dashboards

Contract us

Footprint Website：https://www.footprint.network/
Discord：https://discord.gg/3HYaR6USM7
Twitter: https://twitter.com/Footprint_DeFi
Email: sales@footprint.network