SharkTeam

Annual Web3 Security Report 2022

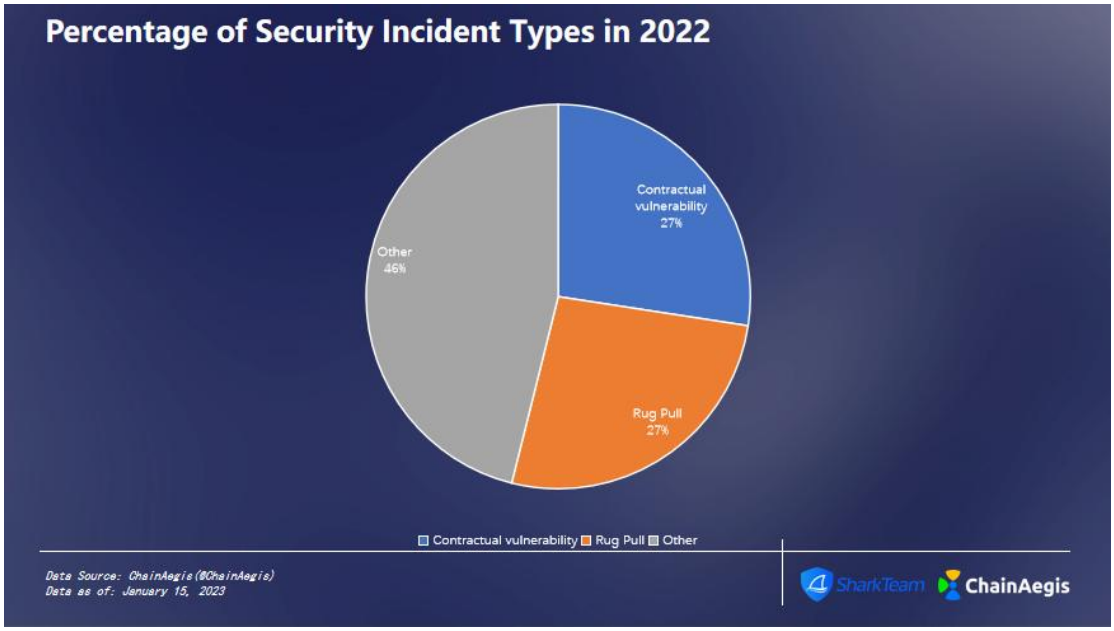
Jan 16, 2023

SharkTeam, a leading blockchain security service team, offers smart contract audit services for developers. To satisfy the demands of different clients, thesmart contract audit services provide both manual auditing and automated auditing.

We implement almost 200 auditing contents that cover four aspects: high-level language layer, virtual machine layer, blockchain layer, and business logiclayer, ensuring that smart contracts are completely guaranteed and Safe.

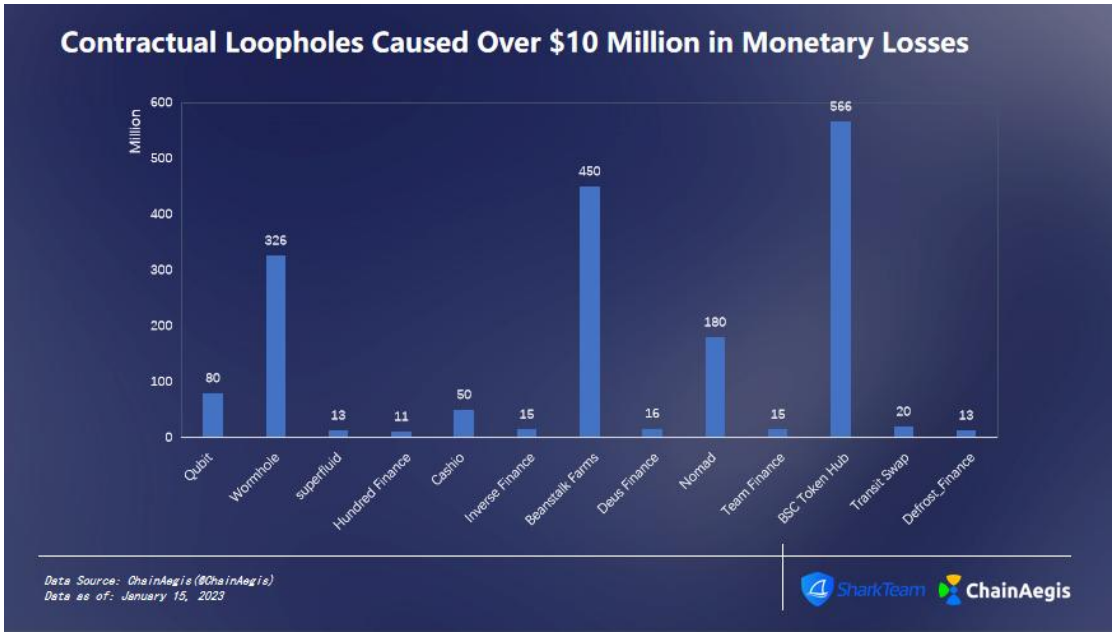
According to the SharkTeam on-chain analytics platform ChainAegis, there were 431 security incidents in the Web3 space in 2022, with an average of 1.2 incidents per day and a total loss of $3.8 billion. Overall, Web3 security incidents remained high throughout 2022, with an annual growth rate of 59.09%, making the overall situation still very challenging.

In FY2022, the proportion of contractual vulnerabilities and Rug Pull incidents remained the same at 27%, while other types of incidents accounted for 46%. The types of security incidents are diverse and the hacking methods are complex, so users need to enhance their security awareness and conduct due diligence on the projects they participate in to avoid being duped. At the same time, project owners should not be complacent and should strengthen their audits of contract security to avoid unnecessary losses due to contract vulnerabilities.



1. Contract Vulnerabilities

In 2022, there were 116 security incidents caused by contractual vulnerabilities, and according to ChainAegis on-chain data, the cumulative loss of funds due to contractual vulnerabilities in 2022 was over $1.7 billion. on 7 October, the BSC Token Hub was hacked. On April 17, Beanstalk Farms was hacked, resulting in a loss of more than RMB 450 million, and on February 3, the cross-chain protocol Wormhole was hacked, resulting in a cumulative loss of 120,000 ETH (approximately USD 320 million). In addition, ChainAegis also counted security incidents with losses of more than $10 million due to contractual vulnerabilities, as follows.

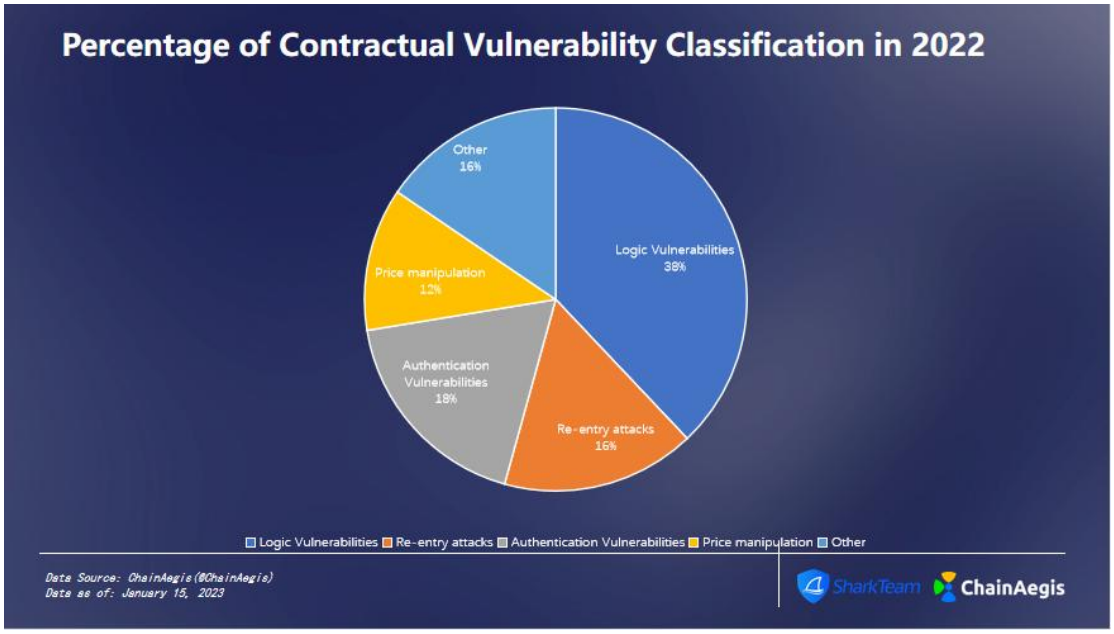


Contract security vulnerabilities in 2022 include: logic vulnerabilities, re-entry attacks, privilege vulnerabilities, price manipulation and others. 38% of security incidents in 2022 were caused by logic vulnerabilities. 8 February saw the hacking of Superfluid, a DeFi protocol on Ether, with losses of over $13 million, which was caused by a logic vulnerability. Logic vulnerabilities can be discovered during the contract security audit phase, and project parties should choose a more professional third-party professional auditor to conduct the audit and reduce the loss caused by contract vulnerabilities.

Permissions vulnerabilities are vulnerabilities in contracts that allow attackers to gain access to user accounts with low privileges and then bypass the privilege checks to steal higher privileges. 18% of security incidents in 2022 were caused by privilege vulnerabilities, and the lack of signature verification in the Wormhole contract during the minting process or the ability of attackers to bypass the verification to mint coins is a privilege vulnerability.

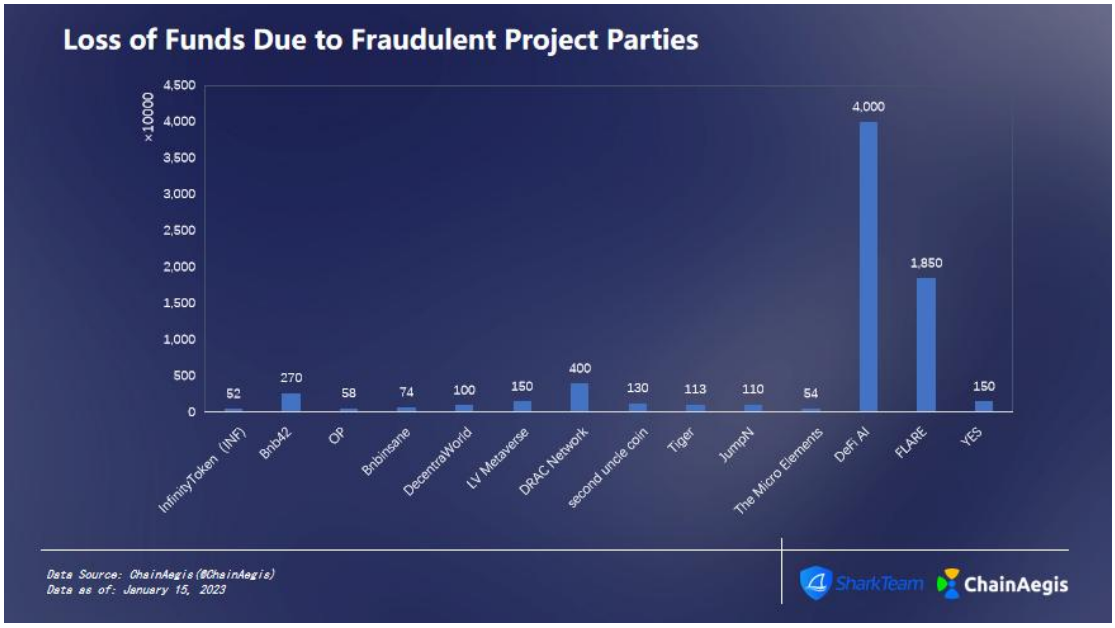
Lightning lending attacks continued to occur, with the main attack techniques that had a significant impact being lightning lending + governance attacks, lightning lending + price manipulation attacks, and lightning lending + re-entry attacks, among others. Price manipulation and re-entry attacks accounted for 12% and 16% of incidents respectively. bDollar was attacked on 21 May for

price manipulation, with the attackers making a profit of 2,381 WBNB (worth approximately US$730,000), while BaconProtocol was hacked on 5 March for a loss of approximately US$958,166, exploiting a re-entry vulnerability and using lightning lending to increase The amount of proceeds. Other types of incidents accounted for 16% of the total, such as the Beanstalk Farms incident (proposal attack).

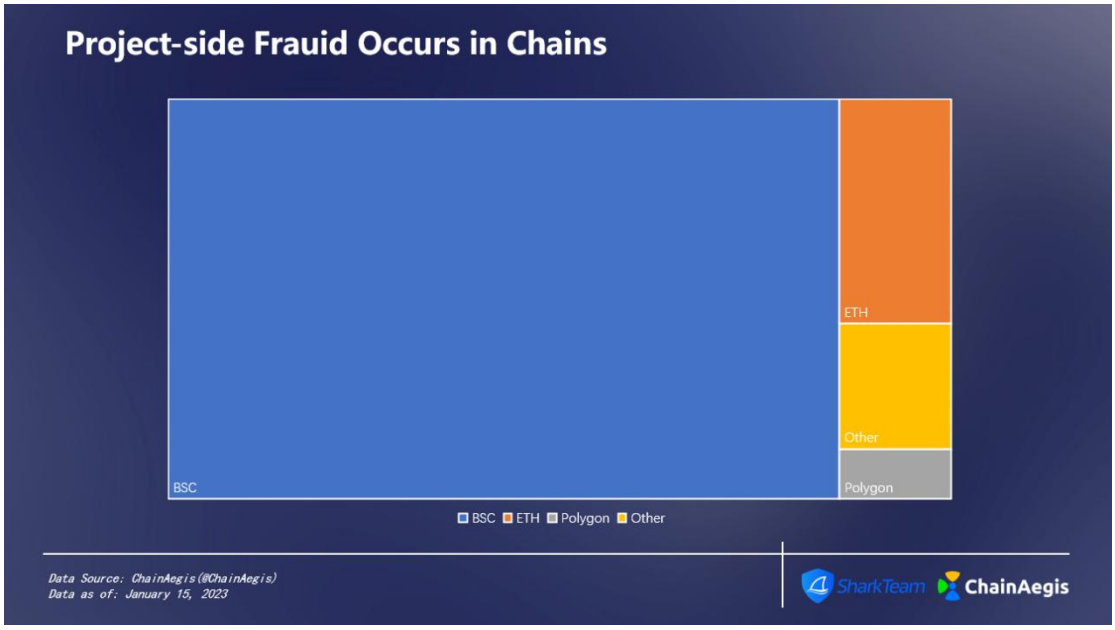


2. Rug pull

There were 112 Rug pull events in 2022, resulting in cumulative financial losses of over $400 million. The largest loss was to the DeFi AI project, with a $40 million Rug pull on November 14.



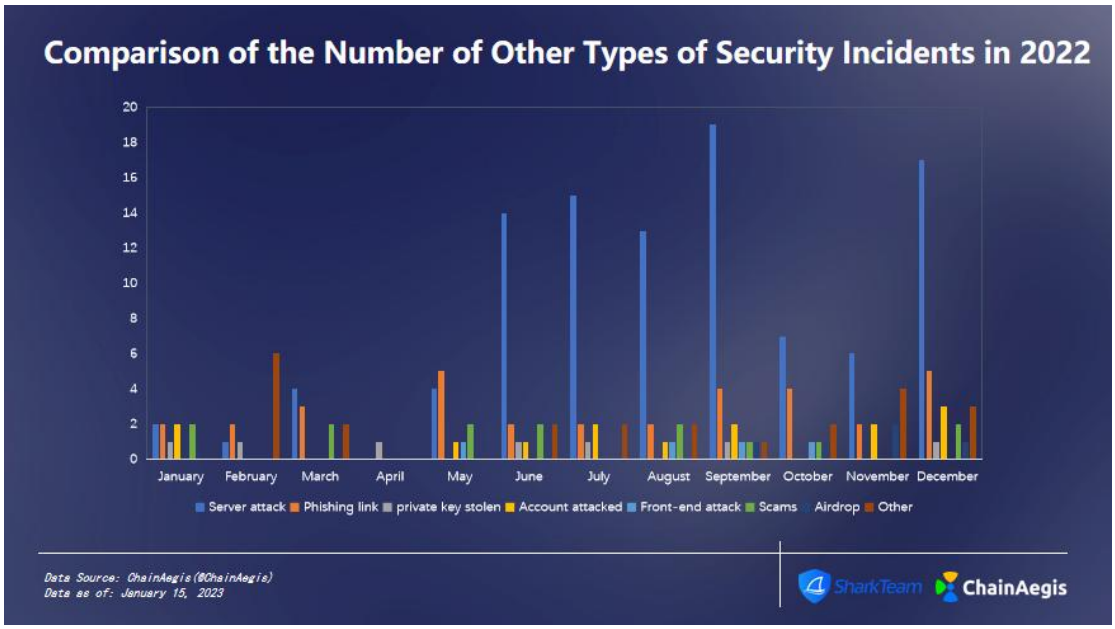
Project-side fraud remains largely focused on the BSC chain, with some occurring on the ETH chain and a few incidents on Polygon and other platforms.

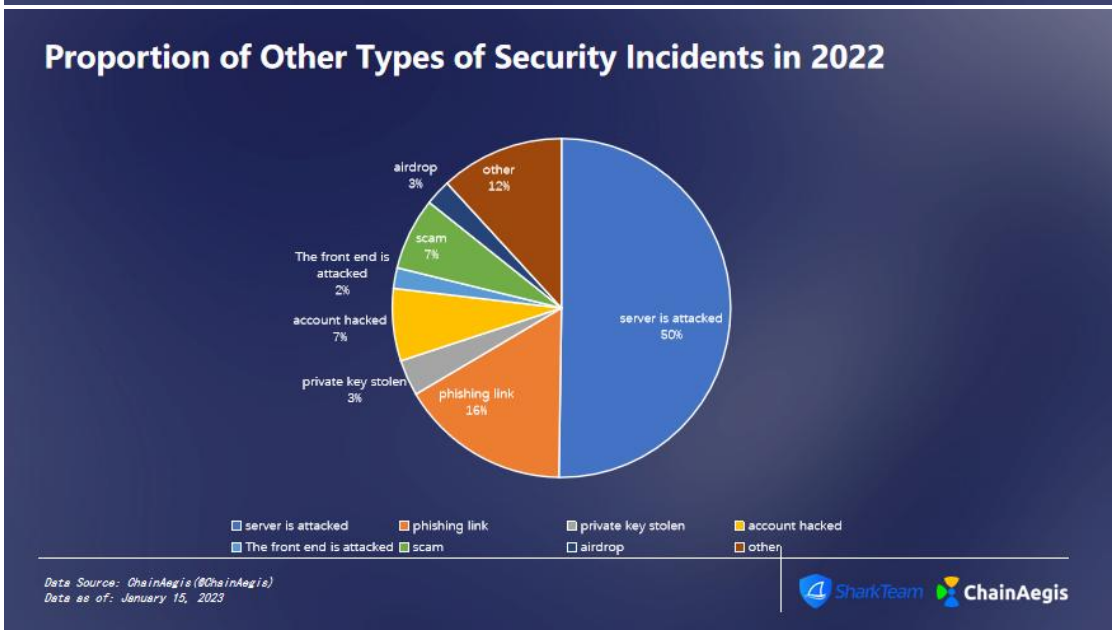


3. Other risks

A total of 203 other types of security incidents occurred in 2022, with server attacks accounting for the largest share at 50%, mainly in the second half of the year, with September having the highest number, accounting for 18.7% of the year, followed by December. Phishing attacks accounted for 16% and

ranked second, with a more even distribution in each month.





On March 18, the official Discord server of the NFT project Rare Bears was attacked.

On March 29, Ronin, the Axie Infinity sidechain, issued a document saying that the verifier node was hacked, and 173,600 ETH and 25.5 million USDC were stolen, with a total amount of about 620 million US dollars.

On May 5, the Cronos ecological DEX MM.Finance was attacked. Hackers used DNS vulnerabilities to steal more than $2 million in CRO Token from users.

On June 9th, http://mint-samsung.com was a phishing website. The phishing site impersonated the Samsung minting site to steal the VeeFriends Series 2 #44451 NFT.

On August 14, Acala issued a document stating that the hacker attack was due to a misconfiguration of the iBTC/aUSD pool, and the transfer of related stolen assets has been prohibited.

On August 25, "Fat Penguin" Pudgy Penguins appeared on the Twitter account @pudgypinguins and the phishing fraud website pudgypengun-lcb[.]com. So far, 22 NFTs have been stolen, including VeeFriends and Pudgy Penguins series NFTs.

On November 2, Deribit, an encrypted derivatives trading platform, announced that its hot wallet was stolen and the funds lost 28 million US dollars. The incident was caused by improper custody of the private key.

The ever-changing and abundant attack methods reflect that the fraud and intrusion methods of hackers and scammers are constantly evolving. Therefore, users must always be in awe of risks, put an end to greed and luck, and be vigilant at all times to avoid asset losses.

About Us

Our vision is to improve security globally. We believe that by building this security barrier, we can significantly improve lives around the world.SharkTeam composes of members with many years of cyber security experiences and blockchain, team members are based in Suzhou, Beijing, Nanjing and Silicon Valley, proficient in the underlying theories of blockchain and smart contracts, and we provide comprehensive services including threat modeling, smart contract auditing, emergency response, etc. SharkTeam has established strategic and long-term cooperations with key players in many areas of the blockchain ecosystem, such as Huobi Global, OKX, polygon, Polkadot, imToken, ChainIDE, etc

Twitter：https://twitter.com/sharkteamorg

Discord：https://discord.gg/jGH9xXCjDZ

Telegram：https://t.me/sharkteamorg

SharkTeam

In Math, We Trust!

https://sharkteam.org

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg