CERTIK

THE BILLION DOLLAR BRIEFING

SEPTEMBER, 2023

Table of Contents

Introduction

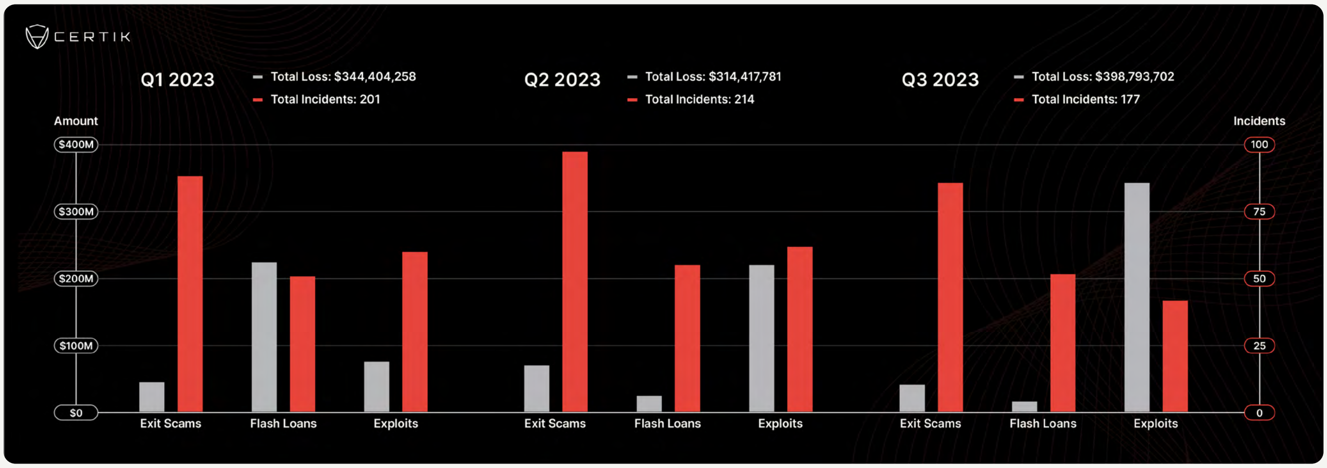
> **This report constitutes a deep dive into the exploits, hacks, and exit scams that have impacted the Web3 community through September 7, 2023 that have contributed to the loss of over $1 billion.**

The Web3 sector reached an unfortunate milestone this week, though it's not exactly unfamiliar territory. As of September 4, 2023, the industry **crossed the $1 billion mark** in terms of value lost to exit scams, exploits, and hacks. In a brighter light, there has been a notable decline in the pace at which funds have been compromised. In 2022, the same billion dollar mark was hit in the month of March. Nevertheless, even if the total losses for 2023 appear to be trending lower, the frequency of incidents mirrors what CertiK documented in 2022. Projecting forward, 2023 could see an escalated number of incidents, albeit with diminished total losses.

Several factors could impact this trajectory, including the prevailing bear market conditions affecting asset valuations, the total value locked (TVL) in DeFi protocols, impending regulatory clarifications, and the potential for large-scale incidents. A significant portion of the 2022 losses can be attributed to breaches orchestrated by nation-state hacking entities, notably the Lazarus group from North Korea. Although Lazarus remained active in 2023, the losses they've inflicted are relatively small compared to 2022. 2023 has seen state-backed hacking factions targeting Web3 platforms without necessarily leading to major financial losses.

To shed light on these evolving trends, we've assembled this report, offering a detailed analysis of the incidents that shape the present security landscape of Web3. We'll delve into various exploit types, classifying them by the tactics and methodologies employed by the entities that carried them out. Additionally, we'll scrutinize the array of exit scams that have been plaguing the sector this year, spotlighting prevalent scam models and prevention techniques. We'll look forward to the rest of 2023 and equip community members with the strategies they need to protect their digital assets in these challenging times.

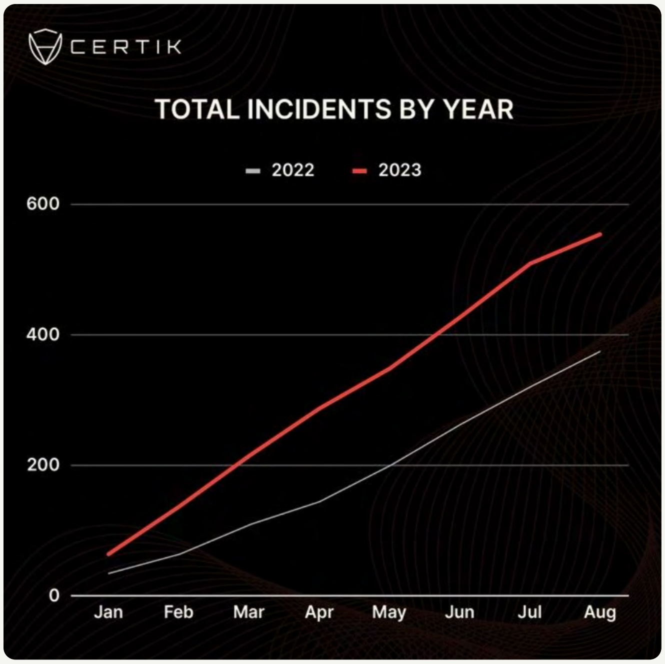
2023 Incident Statistics Summary



Incident Trends Across Chains

Incidents

In 2023, the Web3 sector has witnessed a significant uptick in the number of security incidents. As of now, a total of 576 events have transpired, pushing the average monthly incidents from January through August to 71. This figure presents a marked increase when contrasted with the monthly average of 50 incidents observed in 2022.

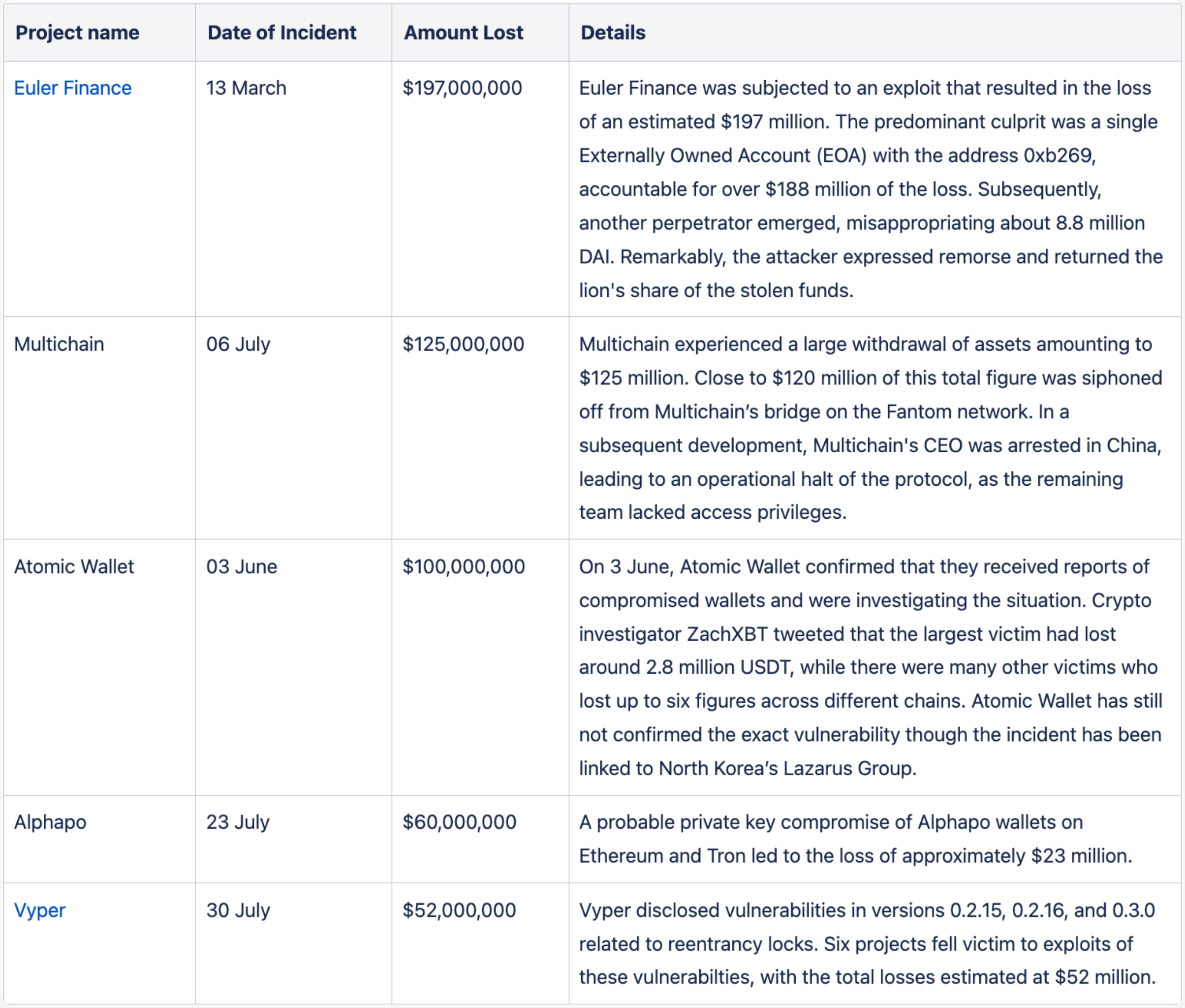


Intriguingly, this surge in incident frequency hasn't been mirrored in terms of financial ramifications. By the same juncture in 2022, the industry losses had already hit $2.4 billion. If the current pattern holds, the financial losses for 2023 could potentially terminate at less than half of the 2022 figures.

Chain Breakdown

A deeper dive into the data uncovers noteworthy trends regarding the platforms most afflicted. Out of the 576 documented incidents, a significant 326 took place on the Binance Smart Chain (BSC), with Ethereum (ETH) trailing at 148.

Together, these two platforms are implicated in a hefty 82% of all recorded incidents. Arbitrum, albeit less frequently targeted, is notable with a count of 25 incidents. Multichain events, predominantly within the realm of decentralized finance (DeFi) lending pools, accounted for 21 incidents.



Project name	Date of Incident	Amount Lost	Details
Euler Finance	13 March	$197,000,000	Euler Finance was subjected to an exploit that resulted in the loss of an estimated $197 million. The predominant culprit was a single Externally Owned Account (EOA) with the address 0xb269, accountable for over $188 million of the loss. Subsequently, another perpetrator emerged, misappropriating about 8.8 million DAI. Remarkably, the attacker expressed remorse and returned the lion's share of the stolen funds.
Multichain	06 July	$125,000,000	Multichain experienced a large withdrawal of assets amounting to $125 million. Close to $120 million of this total figure was siphoned off from Multichain's bridge on the Fantom network. In a subsequent development, Multichain's CEO was arrested in China, leading to an operational halt of the protocol, as the remaining team lacked access privileges.
Atomic Wallet	03 June	$100,000,000	On 3 June, Atomic Wallet confirmed that they received reports of compromised wallets and were investigating the situation. Crypto investigator ZachXBT tweeted that the largest victim had lost around 2.8 million USDT, while there were many other victims who lost up to six figures across different chains. Atomic Wallet has still not confirmed the exact vulnerability though the incident has been linked to North Korea's Lazarus Group.
Alphapo	23 July	$60,000,000	A probable private key compromise of Alphapo wallets on Ethereum and Tron led to the loss of approximately $23 million.
Vyper	30 July	$52,000,000	Vyper disclosed vulnerabilities in versions 0.2.15, 0.2.16, and 0.3.0 related to reentrancy locks. Six projects fell victim to exploits of these vulnerabilties, with the total losses estimated at $52 million.

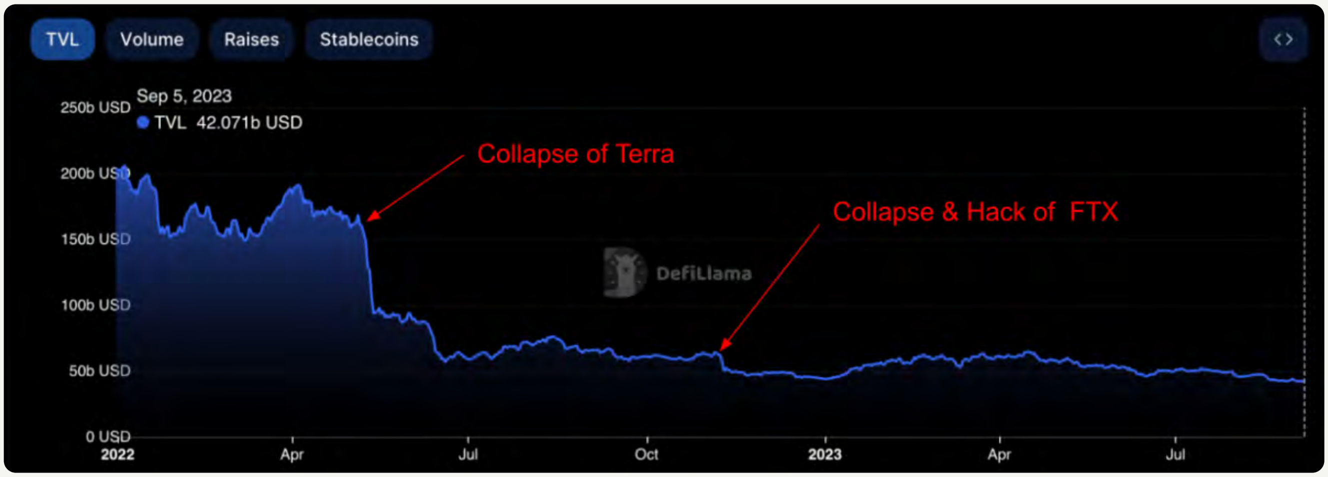
What's Happened so Far This Year?

At the beginning of 2023, CertiK anticipated that despite the ongoing bear market, the Web3 industry would not witness a decline in security incidents. As the year progressed, this prediction held true. By September 2023, CertiK recorded 577 incidents, a number close to the entire count of 607 incidents in 2022. However, one silver lining is evident: the overall financial damage from these incidents has been less severe in 2023 compared to the previous year.

Several factors contribute to this discrepancy in financial impact:

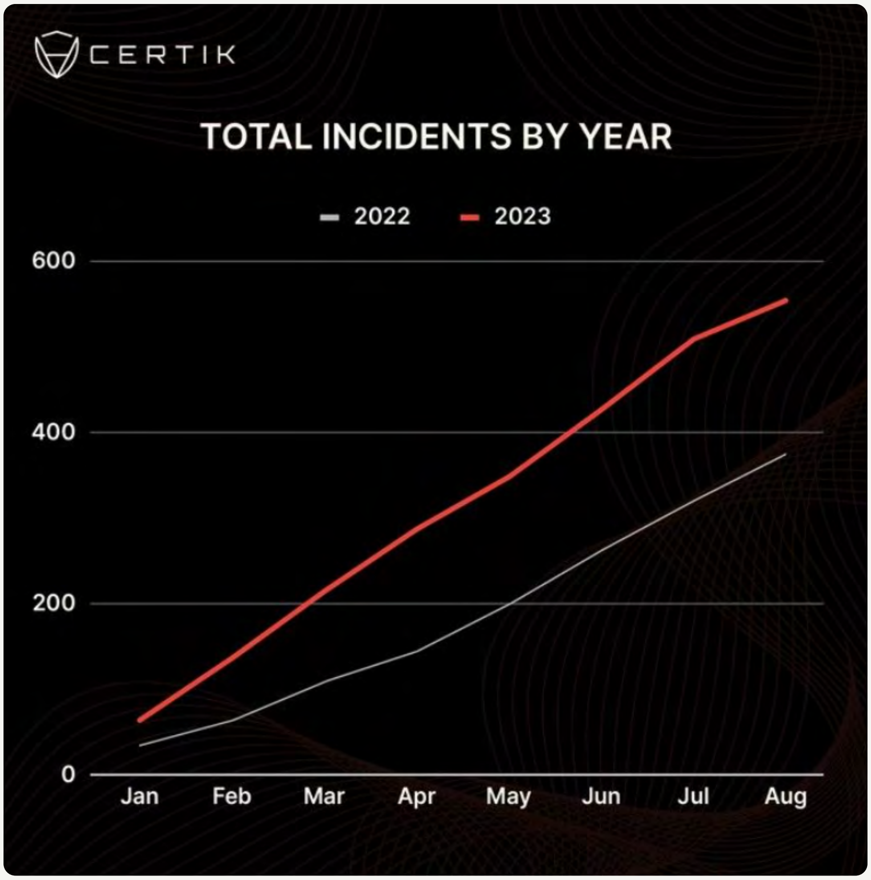
1. Bear Market Impact: The ongoing bear market has led to decreased asset valuations, implying that even when assets are stolen or compromised, their USD equivalent is significantly less than what it would have been during a bullish trend.

2. Reduced Total Value Locked (TVL): DeFi platforms, traditionally lucrative targets for malevolent actors, have seen a drop in the total assets locked. Contributing to this decline is the bear market and the downfall of significant entities, such as FTX. Data from DeFi Llama illustrates this trend, indicating that 2023's TVL has not crossed approximately $65 billion, a stark contrast to the early 2022 peak of $205 billion.



Time to $1 Billion

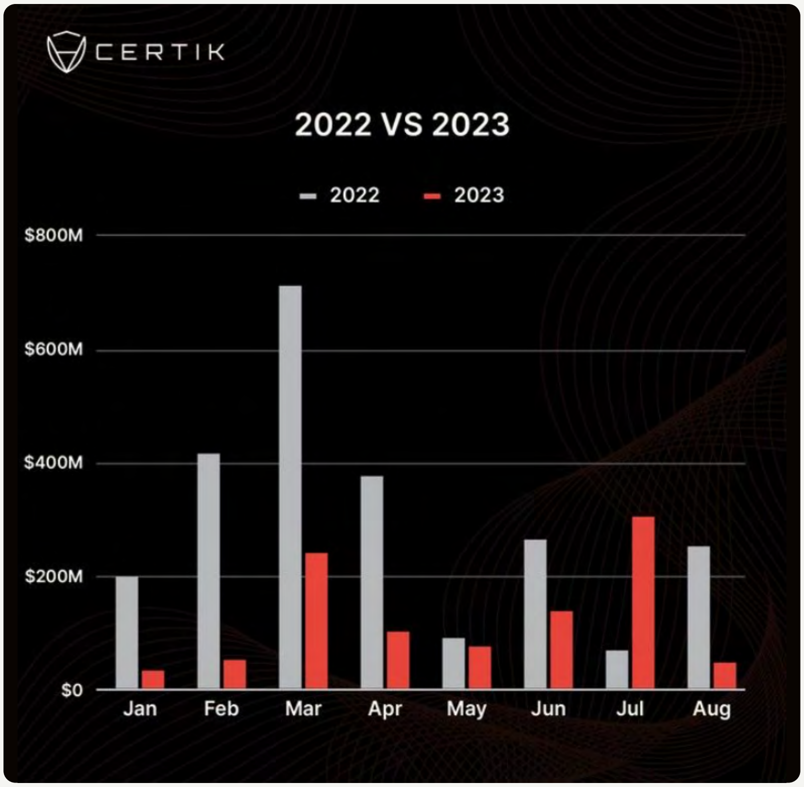
In 2022, $1 billion was lost through scams, hacks, and exploits by March of 2022. This was largely due to the Ronin Bridge exploit in which North Korean hackers stole approximately $624 million. However, in 2023 It has taken until September with the private key compromise of Stake.com wallets to surpass $1 billion lost to hacks, scams and exploits. The two largest incidents in 2022, Ronin and FTX (approximately $477 million) were enough to cover $1 billion in losses between them. In contrast, it has taken 8 months to see similar losses in 2023 and a combined total 571 incidents to surpass $1 billion.



2023 Incidents Summary

In 2022, the crypto community faced numerous setbacks. By the close of the year, bad actors had siphoned off about $3.8 billion in 607 separate incidents. This loss tally hit the $1 billion mark notably earlier in 2022, chiefly because of two significant breaches: the Wormhole exploit in February causing $326 million in damages and the Ronin bridge compromise in March leading to $624 million in losses, totaling a combined $950 million. Of these, the Ronin Network breach stood out as the year's most significant, while Beanstalk Farms reported the heaviest loss from a flashloan attack, amounting to $182.2 million.

Fast forward to 5 September, 2023 and our analysis of the year shows a total of 607 incidents, resulting in a collective loss of $1.03 billion. For comparison, in 2022, the $1 billion threshold was reached with just two major events.

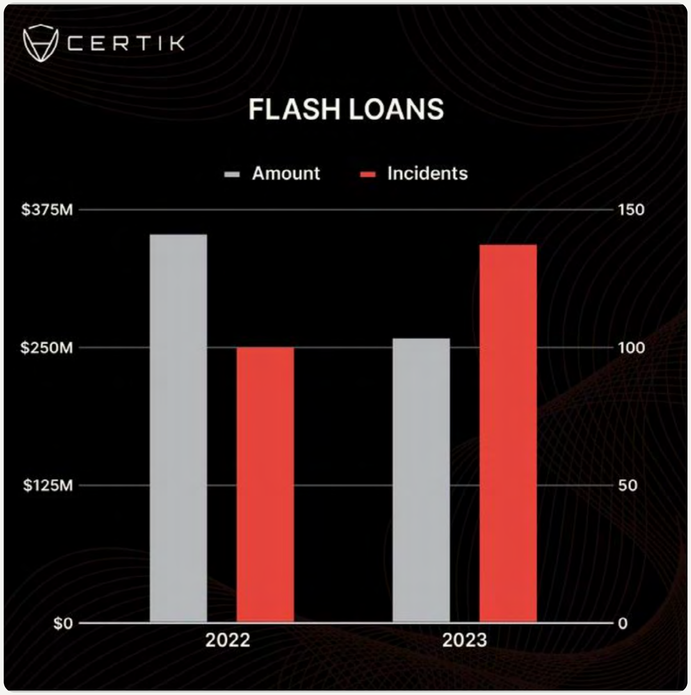


2023’s most significant breach so far is the Euler Finance flashloan attack on 13 March, which led to a $197 million loss. By comparison, 2022 had four breaches that each surpassed this magnitude. A month-by-month analysis for 2023 reveals that March, April, June, and July each registered losses beyond $100 million. Among these, July was particularly harsh, with total losses amassing $303.7 million across various scams, exploits, and breaches.

A comparative assessment between 2022’s major incidents and 2023’s shows a noticeable drop in total losses this year. The starkness of this decline is evident when contrasting the Ronin Network’s $427 million excess loss compared to 2023’s heaviest blow, the Euler Finance incident. The magnitude of breaches in 2022 pushed its average loss per incident to $6.1 million, whereas 2023 averages a more modest $1.8 million. By August’s end in 2022, only 372 incidents had been reported. With 576 incidents by the same time in 2023, it’s clear that while the frequency of incidents has increased, their individual financial impact has decreased.

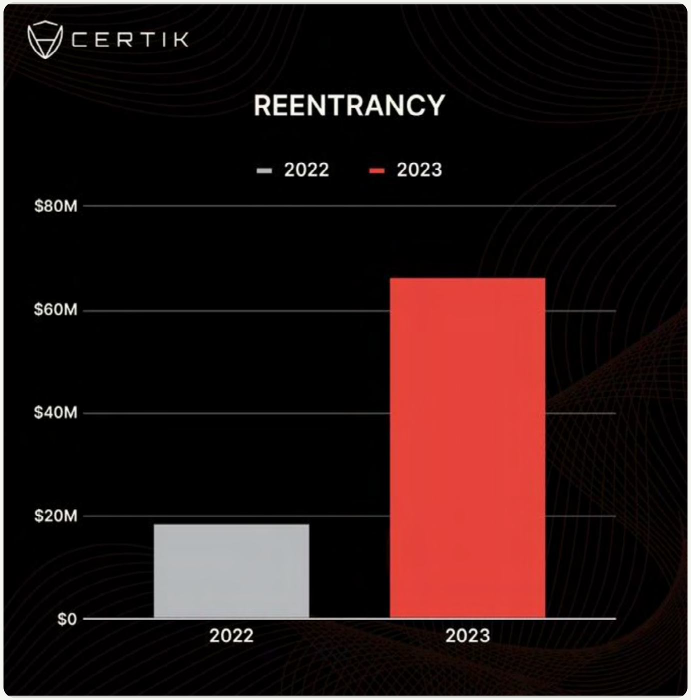
Flashloan Attacks

Flashloan attacks have rapidly become one of the most lucrative avenues for malicious actors targeting the Web3 ecosystem. Since the beginning of our data-keeping in 2020, we've documented 295 such attacks, cumulatively siphoning off over $1.09 billion. High-profile breaches, like the $182 million Beanstalk Farms incident in 2022 and this year's Euler Finance attack, underscore the momentum behind these strategies. Statistically, flashloan attacks represent the second most prevalent type of attack. Generally, these attacks are grouped into three categories: reentrancy, price manipulation, and smart contract code vulnerabilities.

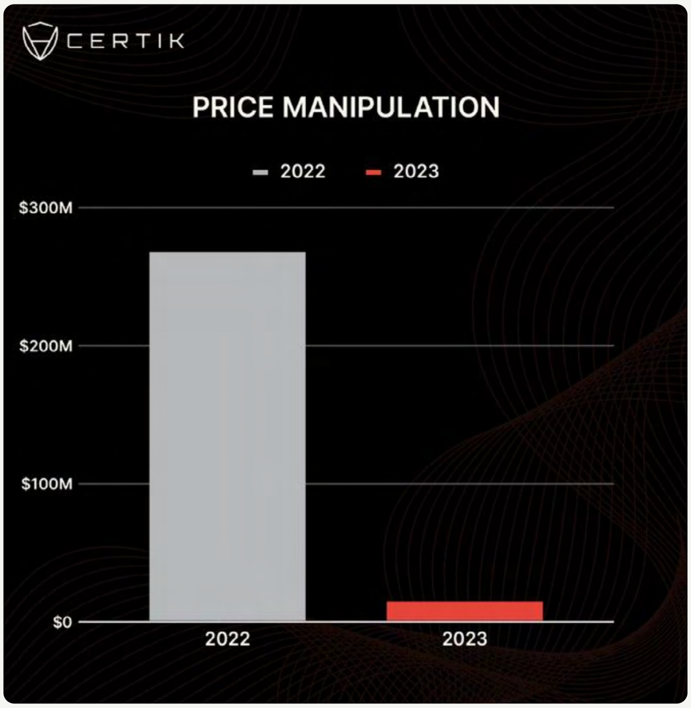


Reentrancy Vulnerabilities

Reentrancy vulnerabilities have precipitated losses of nearly $1 billion. Here, attackers manipulate a bug in a smart contract, allowing them repeated interaction with the contract before its state updates. Consequently, they can divert funds before the contract detects the reduced balance. Despite advances in strengthening smart contract security, these vulnerabilities persist. This predicament underscores the significance of thorough smart contract audits in building a more secure ecosystem.



Price Manipulation



This strategy typically involves artificially manipulating the price of a particular asset, leveraging the resulting market chaos. To execute this, attackers exploit weak points in decentralized exchanges or price oracles. A case in point is the August 2023 breach on Zunami Protocol. The exploiter manipulated StakeDAO's price on Sushiswap using a flashloan. The price on Sushiswap was used to calculate the value of Zunami's UZD stablecoin. The exploiter then moved all the funds – approximately $2.6 million – gained from the exploit to their wallet using Tornado Cash. While Zunami acknowledged the breach, they assured users that the platform's collateral remained secure.

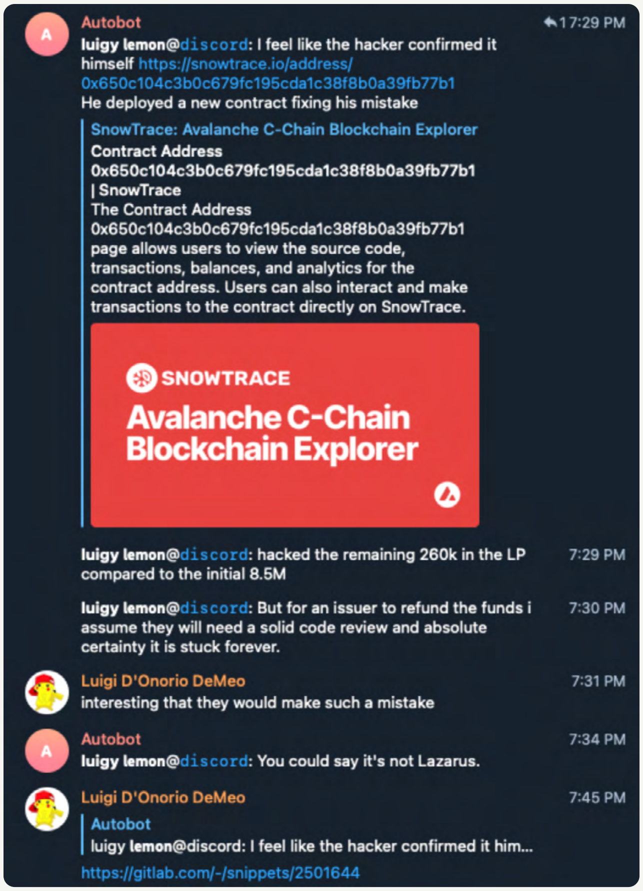
Other Smart Contract Code Vulnerabilities

Smart contract vulnerabilities are a significant Achilles' heel in the Web3 world. At their core, these vulnerabilities typically arise from coding oversights, insufficient testing, or the absence of a comprehensive security review. The fallout from such weaknesses can be serious, ranging from unauthorized fund extraction and contract paralysis to the inadvertent triggering of unintended operations.

The continuous exploitation of such vulnerabilities underlines the need for comprehensive audits, consistent surveillance, and a collective drive towards refining the security standards of smart contracts.

CertiK's records since 2020 reveal that about 395 incidents can be directly attributed to smart contract code vulnerabilities. In 2023, this tally stands at 134. One particularly impactful exploit in this category occurred in February 2023, targeting Platypus DeFi's USP token, when CertiK's monitoring systems flagged an anomalous flashloan transaction linked to this token. The community swiftly flagged the breach in the ETHSecurity Community Telegram channel.

The Platypus DeFi team, after initially shutting down their Telegram and Discord channels in the aftermath of the exploit, later reinstated both platforms. The attacker minted over $40 million of the USP token from the MasterPlatypusV4 contract. They utilized 44 million Platypus LP-USDC tokens as collateral for this minting operation. Subsequently, the attacker called the emergencyWithdraw() function to extract the entirety of the collateral. The final phase of this exploit saw the attacker exchanging all 40 million USP for various stablecoins using the PlatypusV4 pools.



Autobot 17:29 PM
luigy lemon@discord: I feel like the hacker confirmed it himself https://snowtrace.io/address/0x650c104c3b0c679fc195cda1c38f8b0a39fb77b1
He deployed a new contract fixing his mistake

> SnowTrace: Avalanche C-Chain Blockchain Explorer
> Contract Address 0x650c104c3b0c679fc195cda1c38f8b0a39fb77b1 | SnowTrace
> The Contract Address 0x650c104c3b0c679fc195cda1c38f8b0a39fb77b1 page allows users to view the source code, transactions, balances, and analytics for the contract address. Users can also interact and make transactions to the contract directly on SnowTrace.

luigy lemon@discord: hacked the remaining 260k in the LP compared to the initial 8.5M 7:29 PM

luigy lemon@discord: But for an issuer to refund the funds i assume they will need a solid code review and absolute certainty it is stuck forever. 7:30 PM

Luigi D'Onorio DeMeo 7:31 PM
interesting that they would make such a mistake

Autobot 7:34 PM
luigy lemon@discord: You could say it's not Lazarus.

Luigi D'Onorio DeMeo 7:45 PM

> Autobot
> luigy lemon@discord: I feel like the hacker confirmed it him...

https://gitlab.com/-/snippets/2501644

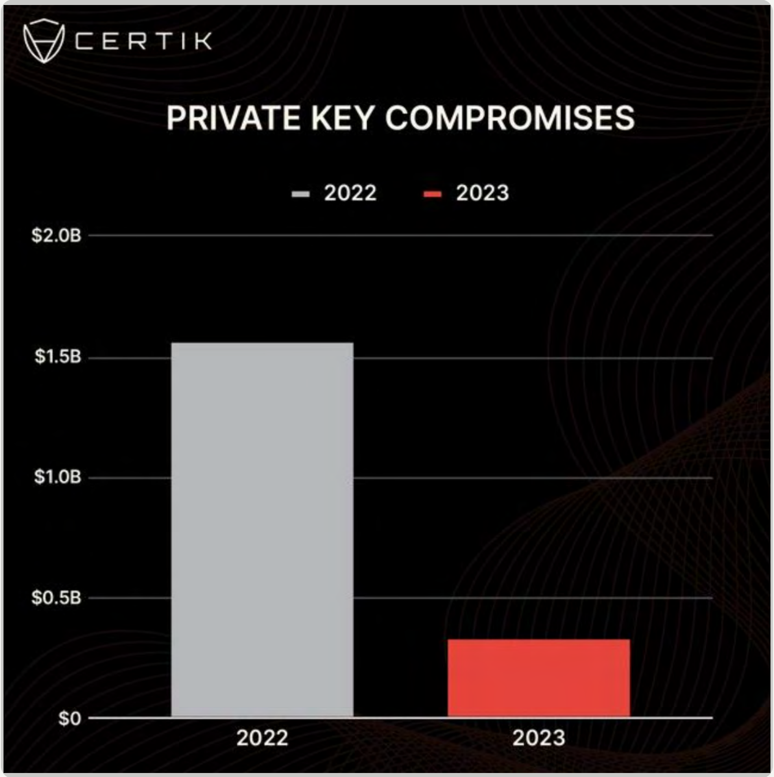
At the heart of this exploit lay a vulnerability in the emergencyWithdraw function's validation mechanism within the MasterPlatypusV4 contract. This validation merely ensured that a user's borrowed assets did not surpass the designated borrowing limit before initiating the transfer of a user's entire deposited assets. It did not take into account the precise quantity of assets a user had borrowed. By exploiting this oversight, the attacker was able to borrow up to the specified borrowing limit, then utilize the emergencyWithdraw function to drain all assets from all depositors, ending up with a total of $9 million in assets.

Private Key Compromises

During the bear market, private key breaches have caused significant financial losses. In 2022, four major breaches led to 38% of the total losses, while so far in 2023 they have accounted for 35%. Even though the total loss in 2023 was lower than 2022, some incidents had exceptionally high losses.

The most striking case is Multichain Protocol. The platform suffered a breach with unauthorized withdrawals totaling over $125 million. Multichain shut down, and their CEO was arrested in China. The platform's MPC keys were lost, leaving assets irretrievable. Later, the CEO's sister was arrested, on suspicion of having moved funds to her accounts.

This breach affected multiple networks including Fantom, Dogecoin, and Moon River. The attacker may have exploited or gained access to Multichain's multi-party computation (MPC) system. With the CEO's sudden absence and other technical glitches, there were whispers of an inside job. This led Binance to drop support for several Multichain-bridged tokens.



Phishing

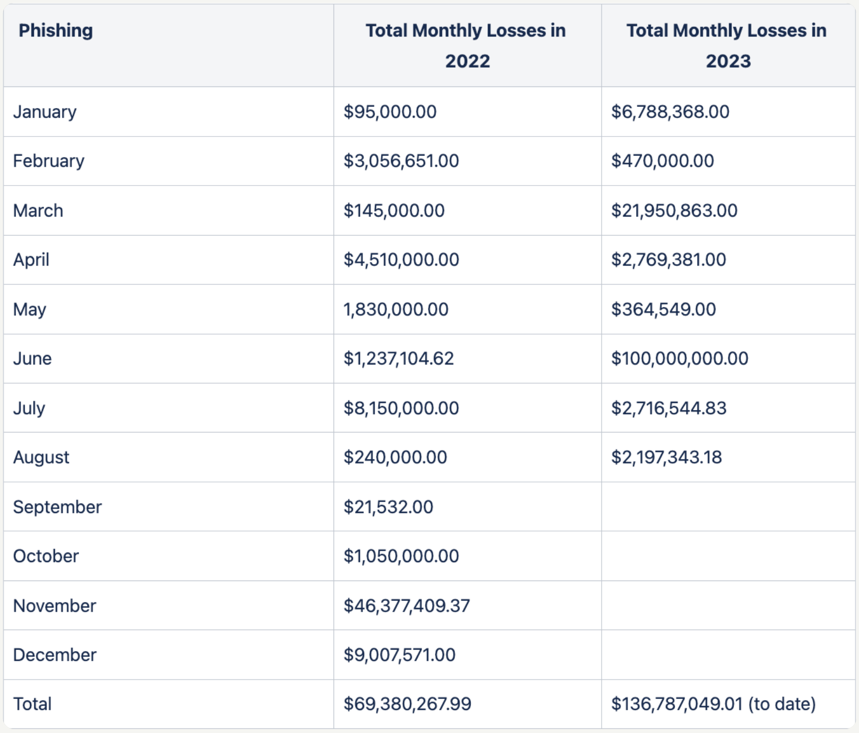
Phishing tricks users into revealing sensitive info like login credentials and wallet details. Attackers use fake sites and tactics to make victims share this data, sometimes even connecting their wallet to a fake browser extension. These schemes may target one person but often aim for broader system access.

A notable case was with Atomic Wallet. This well-known crypto wallet saw a major breach, with hackers taking $35 to $100 million in tokens from its users, impacting roughly 50,000 people, or about 1% of its monthly users.

Several issues played a role: weak cryptography, scanty documentation, and mishandling the Electron framework. While the breach's root cause is uncertain, potential risks included weak key generation, algorithm issues, keys sent to central servers, and supply chain attacks.

The Lazarus Group, tied to North Korea, is believed to be behind this. The stolen assets were linked to a crypto-mixer, Sinbad, associated with the Lazarus Group.

This event emphasizes crypto's security risks, especially online "hot" wallets. For secure long-term holding, consider offline "cold" storage and stay alert to threats, including phishing.



Phishing	Total Monthly Losses in 2022	Total Monthly Losses in 2023
January	$95,000.00	$6,788,368.00
February	$3,056,651.00	$470,000.00
March	$145,000.00	$21,950,863.00
April	$4,510,000.00	$2,769,381.00
May	1,830,000.00	$364,549.00
June	$1,237,104.62	$100,000,000.00
July	$8,150,000.00	$2,716,544.83
August	$240,000.00	$2,197,343.18
September	$21,532.00	
October	$1,050,000.00	
November	$46,377,409.37	
December	$9,007,571.00	
Total	$69,380,267.99	$136,787,049.01 (to date)

Exit Scams

CertiK has uncovered 269 exit scams to date in 2023, causing a total loss of approximately $138 million for investors. This averages out to a loss of $511,000 per scam. Despite market downturns, exit scams remain a persistent issue for Web3 investors. In the first eight months of 2022, 208 exit scams led to losses of $144.6 million. In the same period in 2023, there were 269 scams with around $136.9 million lost. This rise in 2023 is mainly due to scams mimicking genuine projects and fraudulent initiatives on new chains such as Base, Arbitrum, and zkSync.

One common exit scam is the honeypot, where victims buy tokens they are unable to sell. Many of these are promoted in Telegram groups.

With the excitement around newly-launched chains, investors can be easily lured into fraudulent projects, leading to significant losses.

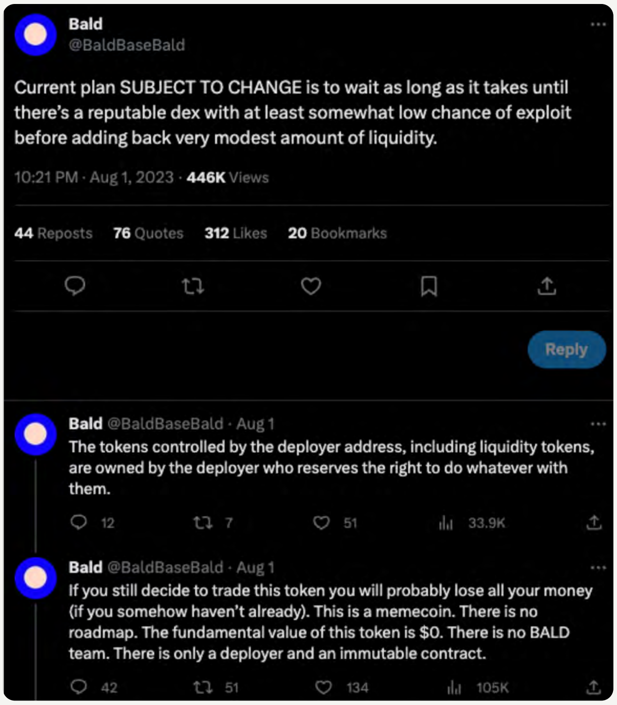
Scam Tokens

Throughout the year, CertiK identified several honeypot tokens mimicking real projects. Their aim? Deceive investors into investing, then pull the liquidity. As major projects like Arbitrum token, zkSync, SUI, and Sei Network launched, scammers rode their coattails, creating fraudulent tokens with similar names.

Classic Exit Scams AKA Rug Pulls

Some of the most significant scams happened on newer blockchains, including Arbitrum and zkSync. Of the 18 major exit scams in 2023, seven were on these new platforms. Newer chains, with their buzz and growing adoption, make attractive hunting grounds for scammers. The infamous $BALD scam on Base exemplifies this.

In July, the $BALD coin deployer on Coinbase’s new BASE blockchain pulled liquidity in several moves, netting roughly 3,163 ETH or around $5.9 million. Interestingly, the token’s agreement did explicitly allow the deployer to perform such actions, pointing to the inherent risks in centralized tokens.



Bald
@BaldBaseBald

Current plan SUBJECT TO CHANGE is to wait as long as it takes until there's a reputable dex with at least somewhat low chance of exploit before adding back very modest amount of liquidity.

10:21 PM · Aug 1, 2023 · 446K Views

44 Reposts 76 Quotes 312 Likes 20 Bookmarks

Bald @BaldBaseBald · Aug 1
The tokens controlled by the deployer address, including liquidity tokens, are owned by the deployer who reserves the right to do whatever with them.

12 7 51 33.9K

Bald @BaldBaseBald · Aug 1
If you still decide to trade this token you will probably lose all your money (if you somehow haven't already). This is a memecoin. There is no roadmap. The fundamental value of this token is $0. There is no BALD team. There is only a deployer and an immutable contract.

42 51 134 105K

On June 27, Chibi Finance carried out a premeditated exit scam. The Chibi Finance team misused centralized controls present in the _gov role within their contracts. Here's a breakdown of the scam:

1. A malicious contract was crafted by the team.

2. Using addPool, this contract was linked to multiple Chibi Finance contracts.

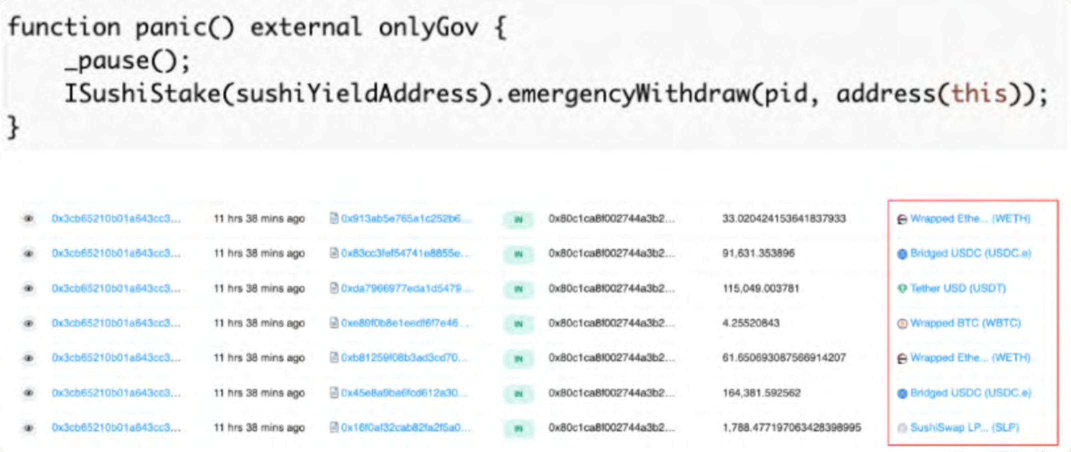
3. The setGov function was then called by the Chibi Finance deployer to assign the _gov role to this malicious contract.

4. With this role, the malicious contract activated the panic function on all linked pools, emptying them.

5. The stolen assets were then converted into ETH.

6. These funds were moved to the Ethereum network and subsequently laundered through Tornado Cash.

This incident underscores the importance of thoroughly understanding contract permissions and roles when interacting with or investing in DeFi projects.



```
function panic() external onlyGov {
    _pause();
    ISushiStake(sushiYieldAddress).emergencyWithdraw(pid, address(this));
}
```

0x3cb65210b01a643cc3...	11 hrs 38 mins ago	0x913ab5e765a1c252b6...	IN	0x80c1ca8f002744a3b2...	33.020424153641837933	Wrapped Ethe... (WETH)
0x3cb65210b01a643cc3...	11 hrs 38 mins ago	0x83cc3fef54741e8855e...	IN	0x80c1ca8f002744a3b2...	91,631.353896	Bridged USDC (USDC.e)
0x3cb65210b01a643cc3...	11 hrs 38 mins ago	0xda7966977eda1d5479...	IN	0x80c1ca8f002744a3b2...	115,049.003781	Tether USD (USDT)
0x3cb65210b01a643cc3...	11 hrs 38 mins ago	0xe89f0b8e1eedf6f7e46...	IN	0x80c1ca8f002744a3b2...	4.25520843	Wrapped BTC (WBTC)
0x3cb65210b01a643cc3...	11 hrs 38 mins ago	0xb81259f08b3ad3cd70...	IN	0x80c1ca8f002744a3b2...	61.650693087566914207	Wrapped Ethe... (WETH)
0x3cb65210b01a643cc3...	11 hrs 38 mins ago	0x45e8a9ba6fcd612a30...	IN	0x80c1ca8f002744a3b2...	164,381.592562	Bridged USDC (USDC.e)
0x3cb65210b01a643cc3...	11 hrs 38 mins ago	0x16f0af32cab82fa2f5a0...	IN	0x80c1ca8f002744a3b2...	1,788.477197063428398995	SushiSwap LP... (SLP)

Funds Lost to Nation State-Backed Actors

In recent years, the Web3 industry has seen an upsurge in attacks, not just from individual scam artists, but also from highly coordinated groups backed by nation-states, known as Advanced Persistent Threats (APTs). These groups, known for their sophistication and persistence, have been responsible for significant losses in the sector. Here, we dissect the trends, incidents, and implications of these activities in 2023.

The prevalence of APTs in the Web3 space isn't a new phenomenon; reports of their activities can be traced back to 2017 or possibly earlier. The Lazarus group, a North Korean APT, has been particularly active, responsible for stealing approximately $1.7 billion in 2022 alone. This group seems to stand as the most active state-backed entity in this sector.

In 2023, the landscape saw fewer confirmed attacks from state-backed groups than previous years. These groups, particularly from North Korea, continue to exhibit adaptability and sophistication, employing tactics such as supply chain attacks to compromise Web3 entities and IT service providers associated with them.

Notable Incidents

Lazarus Group Attacks

- **Alphapo and CoinsPaid Compromises**
  - **Dates:** 22nd and 28th July
  - **Loss:** Alphapo experienced two separate attacks totaling a loss of $60 million, while CoinsPaid lost $37 million.

- **Modus Operandi:** Used signature Lazarus tactics, including social engineering and bribery, and targeted internet-accessible applications.
- **Evidenced Attribution:** Independent investigator ZachXBT first alleged Lazarus' involvement, citing similar on-chain activities linked to the group. These claims are yet to be corroborated by threat intelligence experts.

- **APT43 Emergence**
  - **Dates:** Identified on 29th March.
  - **Objective:** Alleged to utilize stolen funds to fund North Korea's defense operations through cryptocurrency mining.
  - **Attribution:** Identified by Google's threat intelligence division, Mandiant, as a separate entity from Lazarus, though caution still surrounds this designation. This particular APT's goal is alleged to be "buy[ing] hash rental and cloud mining services...which it then uses to mine cryptocurrency."
- **JumpCloud Breach**
  - **Dates:** Reported on 20th July.
  - **Impact:** Less than five customers affected.
  - **Objective:** Believed to target JumpCloud's Web3 clients, although the financial repercussions remain unclear. Likely to have been the work of North Korean-affiliated actors.

Notable Incidents

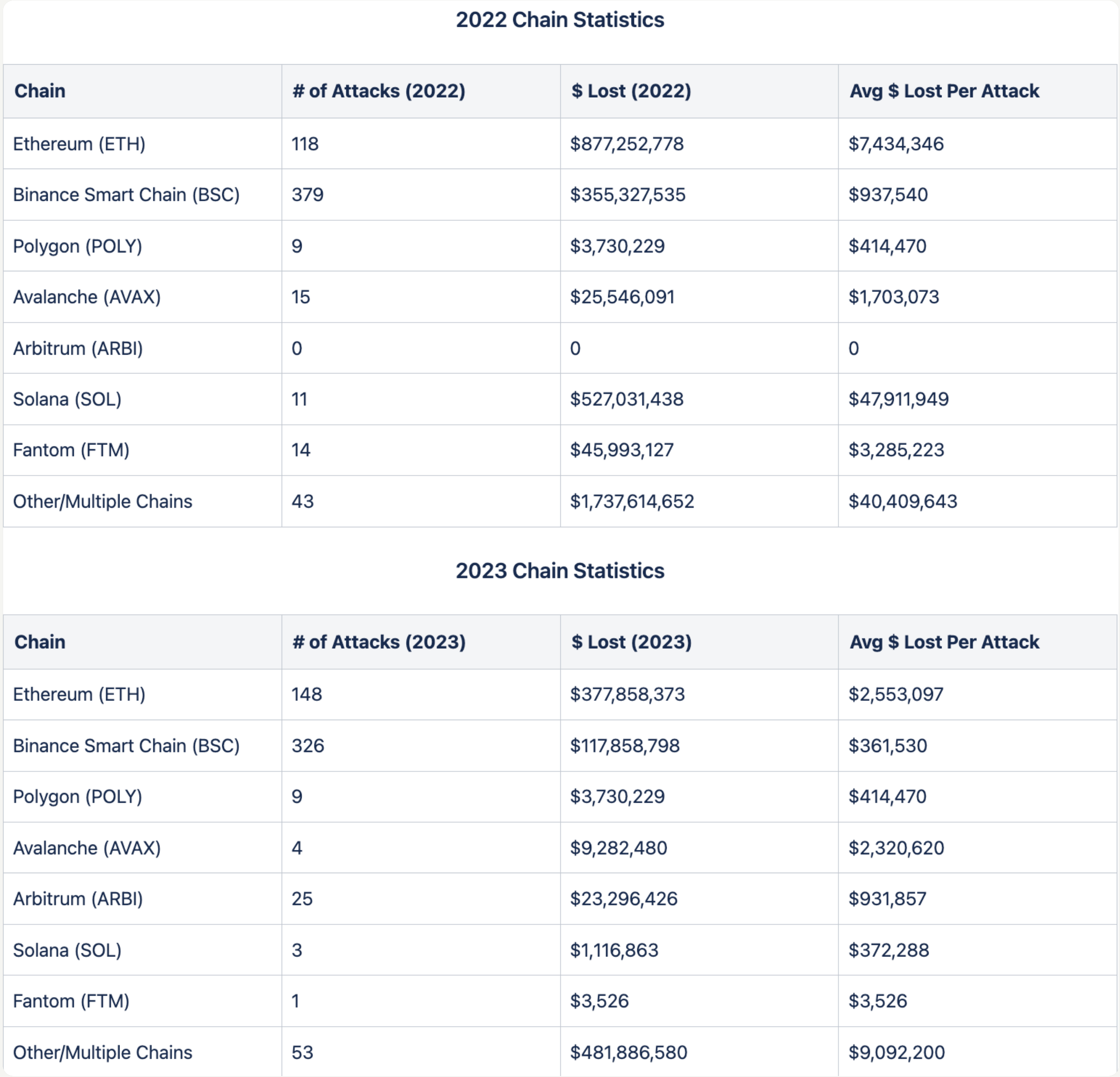
The continual involvement of APTs in the Web3 space signals enduring vulnerabilities and lucrative opportunities within the industry. Particularly concerning is the rise in supply chain attacks, wherein third-party service providers are compromised to deliver malware to the intended targets. Noteworthy are the incidents flagged by Kaspersky involving IT service provider 3CX, with Lazarus as the attributed perpetrator.

Companies in the Web3 space need to be acutely aware of the growing threats and adapt their security measures accordingly. This includes robustly vetting third-party service providers and enhancing internal security protocols to mitigate potential infiltrations.

While 2023 has seen a slight dip in confirmed nation-state-backed cyber activities, the threats remain substantial and are ever-evolving. The emergence of new groups like APT43 and the continued operations of established entities like the Lazarus Group underscore the need for vigilance and adaptive security in the Web3 industry.

Incident Breakdown by Chain

When analyzing different blockchains understanding trends and shifts is crucial. Comparing CertiK's data for losses by chain from 2022 and 2023 provides insight into the number of challenges certain chains face.



2022 Chain Statistics

Chain	# of Attacks (2022)	$ Lost (2022)	Avg $ Lost Per Attack
Ethereum (ETH)	118	$877,252,778	$7,434,346
Binance Smart Chain (BSC)	379	$355,327,535	$937,540
Polygon (POLY)	9	$3,730,229	$414,470
Avalanche (AVAX)	15	$25,546,091	$1,703,073
Arbitrum (ARBI)	0	0	0
Solana (SOL)	11	$527,031,438	$47,911,949
Fantom (FTM)	14	$45,993,127	$3,285,223
Other/Multiple Chains	43	$1,737,614,652	$40,409,643

2023 Chain Statistics

Chain	# of Attacks (2023)	$ Lost (2023)	Avg $ Lost Per Attack
Ethereum (ETH)	148	$377,858,373	$2,553,097
Binance Smart Chain (BSC)	326	$117,858,798	$361,530
Polygon (POLY)	9	$3,730,229	$414,470
Avalanche (AVAX)	4	$9,282,480	$2,320,620
Arbitrum (ARBI)	25	$23,296,426	$931,857
Solana (SOL)	3	$1,116,863	$372,288
Fantom (FTM)	1	$3,526	$3,526
Other/Multiple Chains	53	$481,886,580	$9,092,200

Understanding the dynamics of security trends within the blockchain ecosystem is vital, especially when the industry is in a rapid phase of growth and transformation.

Ethereum (ETH) and Binance Smart Chain (BSC)

- **Year-over-Year Comparison:**
  - **Ethereum:** Losses dropped from $877 million in 2022 to $377.9 million in 2023.
  - **Binance Smart Chain:** Losses decreased from $355 million in 2022 to $115.7 million in 2023.

Fantom (FTM) and Solana (SOL)

- Both chains experienced a decrease in the number of attacks and the associated financial losses. Their evolution mirrors that of Ethereum and BSC. The decline in attacks and losses could stem from a combination of factors such as improved security awareness among developers and users, advancements in threat detection and prevention tools, a rise in smart contract auditing, and declines in token values and TVL.

Avalanche (AVAX) and Arbitrum (ARBI)

- These networks had fewer attacks but saw higher average losses per incident. This suggests a strategic targeting by cybercriminals, viewing these chains as potentially more lucrative for their endeavors.

The diverse landscape of the Web3 ecosystem means threats can emerge from unexpected quarters. As innovation surges forward, the stakes get higher, underlining the importance of rigorous security measures. Smart contract auditing, continuous monitoring, advanced threat detection tools, and a proactive security culture will be the cornerstones of a safe and robust blockchain environment moving forward.

Cross-chain Bridges

It is noteworthy that bridge contract exploits lead to particularly big losses. In 2022 bridge exploits led to over $2 billion losses, accounting for over half of the total losses for the year. In 2023, the second largest attack is targeted Multichain where $125 million was lost after the CEO were held custody in China and the protocol shut down as the rest of the team lost access. PolyNetwork, which also lost $5 million, is another notable victim in this regard.

A multi-chain cryptoverse is now a reality and bridge protocols that allows users to transfer crypto across these chains plays an increasingly important role in the broader ecosystem.

In general, cross-chain bridges are more centralized and less transparent than other types of DeFi projects which presents their own unique set of risks.

Centralization

A common feature in the bridge protocol design are the central storage points of funds on both the source chain that receives initial tokens from users and on target chain that releases bridged assets. Whether the funds are locked up in a smart contract or held by a custodian, the address itself is a single point of failure of all the funds in bridge protocols and particularly attractive targets for exploiters. Any compromise to those addresses, be it private key compromise or code exploit vulnerabillities would lead to much larger losses than a DEX, for example.

Less Transparency of External Validation

Bridges rely on validators to verify and processing cross-chain transactions. While other DeFi logic are confined by on-chain smart contracts, bridge validation processes are sometimes done externally. This new layer optimized for speed and cost but introduce new opaque risk factors. Notably Multichain implemented its own Multi-Party Computation (MPC) network of validators for verifying and signing transactions. The bridge experienced $130 million of allegedly unauthorized withdrawals, promptly followed by the arrest of the CEO by Chinese police in June yet the community only confirmed it much later.

Noteworthy Regulatory Actions in 2023

- The U.S. Securities and Exchange Commission (SEC) pursued legal action against Binance, Coinbase, Bittrex, TerraUSD, and Ripple Labs.

- The International Organization of Securities Commissions (IOSCO) unveiled a global approach to regulating digital markets after FTX’s collapse in 2022. The framework seeks strengthened cooperation among members, aiming to better protect investors and deter non-compliance.

- The International Monetary Fund (IMF) proposed five key recommendations for global digital asset regulation:

    - » It is advised that crypto asset service providers be licensed, registered, and authorized.
    - » Any entities carrying out multiple functions should be subjected to additional prudential requirements.
    - » Issuers of stablecoins should also be subjected to strict prudential requirements.
    - » Regulated financial institutions should have clear requirements to meet, concerning their exposure and engagement with cryptocurrency.
    - » The international community will eventually need robust, comprehensive, globally consistent crypto regulation and supervision.

- The Group of Twenty (G20) nations, in collaboration with the IMF and Financial Stability Board (FSB), are slated to release a Global Crypto Policy Roadmap, on global crypto regulations, focusing on global macro implications. This will be presented before the G20 Leaders' Summit in September.

Japan's Proactive Approach to Web3

Japan has actively integrated cryptocurrency through regulations, recognizing blockchain and Non-Fungible Tokens as vehicles for economic growth. This strategy was effective as FTX Japan investors were shielded from FTX's fallout due to the Financial Services Agency (FSA) mandate of 95% of consumer crypto assets being in cold wallets. Japan also instituted the "travel rule" in June 2023, obligating financial institutions to disclose customer information for crypto transfers exceeding $3,000. This has garnered support from the Group of Seven (G7) committee.

Security Beyond Consumer Protection

The cloak of (pseudo-)anonymity provided by cryptocurrencies has been exploited for funding malicious geopolitical activities. In June 2023, Israel seized millions from wallets believed to finance the Iranian military and Hezbollah.

Case Study: Tornado Cash

The U.S. Department of Justice charged the developers of Tornado Cash in August 2023 for aiding North Korea's Lazarus Group in laundering almost $1 billion from crypto breaches. A U.S. judge ruled that the U.S. Treasury Department acted within its jurisdiction when sanctioning Tornado Cash in 2022. The judge affirmed the ban on U.S. persons from using Tornado Cash and supported the U.S. Treasury's Foreign Assets Control's proper designation of the exchange due to its exploitation by North Korea's Lazarus group.

Future Predictions

Due to the bear market conditions we're unlikely to see a significant uptick in the amount of funds lost to scams or exploits even if the volume of such instances remains high. This is mainly because asset prices and the TVL have significantly fallen since the start of 2022. The exception to this trend would highly likely come in the form of additional private key compromises on crypto companies that hold a large amount of assets.

With the exception of the Euler Finance flash loan, the largest incidents in 2023 have come in the form of private key compromises. Incidents such as the Poly Network attack, Multichain, Alphapo, Coinspaid and Stake were all due to private key compromises and have led to combined losses of $363.3 million, just over a third of the overall funds lost in 2023. Additionally $1.4 billion was lost to private key compromises in 2022, accounting for 38% of the overall amount lost in 2022.

Flash loans, exploits and exit scams will continue to plague the Web3 ecosystem, however private key compromises will highly likely continue to pose the greatest challenge to the Web3 industry. July in 2023 saw losses comparable to those seen in the first and second quarter of the year which can be attributed to private key compromises on Multichain, Alphapo, Coinspaid and Poly Network. For the remainder of the year, months that have losses comparable to losses in an entire quarter will likely be due to private key compromises. This trend will likely continue until we see bull market trends reappear.

Conclusion

Nearly three-quarters of the way into 2023, we can discern a distinctive shift from 2022. Total losses took six months longer to reach the $1 billion mark in 2023 compared to 2022. Despite a spike in the number of security incidents this year, total losses have been notably reduced. This is (hopefully) attributable to improved security measures taken by Web3 teams and users, but is likely to be strongly influenced by the decline is asset valuations over the last 18 months.

Meanwhile, the jury is still out on whether or not a global regulation framework will evolve in the years to come, but what's indisputable is the increasing pressure on governments and financial bodies worldwide to address the challenges and potential of the Web3 landscape. Public and private sector firms are acknowledging the value of collaboration in this domain. Industry-led self-regulatory initiatives, combined with government oversight, could provide a viable path forward. Such an approach would allow for industry-specific knowledge to inform the rule-making process while ensuring that the overarching principles of investor protection and financial stability are upheld.

In addition, as more traditional financial institutions venture into the crypto and Web3 spaces, their expertise and practices can offer valuable insights into how regulations could be tailored. Similarly, the experiences and learnings from early adopters and pioneers in the crypto space will be crucial in informing regulatory decisions.

Ultimately, while a global regulatory framework might remain elusive in the near term due to the myriad of perspectives and priorities among nations, the convergence of localized best practices might offer a blueprint for broader international collaboration in the future. This potential paradigm shift would be integral in ensuring that the Web3 ecosystem remains secure, resilient, and primed for sustainable growth.

CERTIK

Securing the **Web3** World