CERTIK

HACK3D

THE WEB3 SECURITY REPORT

2024

Elevating Your Entire Web3 Journey

Table of Contents

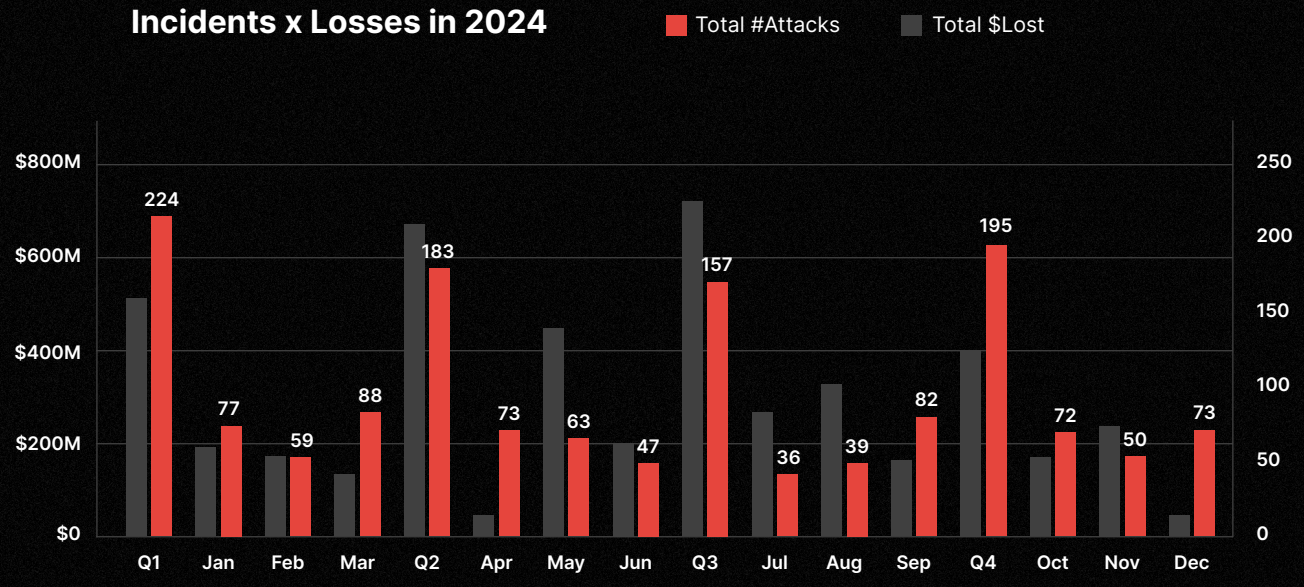
Executive Summary

- A total of **$2,362,748,975.83** was lost across **760** on-chain security incidents in 2024.
- These figures represent an approximate **31.61%** increase in value stolen compared to 2023. The number of security incidents year-over-year, however, decreased by **29**.
- The average amount lost per hack in 2024 was **$3,108,880** (a **23.04%** increase from the previous year), and the median amount stolen was **$150,925** (a **46.83%** year-over-year increase).
- May was the most costly month of the year, with **$444,386,754** lost across **63** incidents.
- Similar to Q3 of 2023, Q3 of 2024 saw the most losses, with **$753,301,497** stolen in **157** hacks, scams, and exploits. The subsequent quarter saw a **46.65%** decline in the amount stolen.
- Phishing was the most costly attack vector in 2024, with **$1,050,129,498** lost across **296** incidents, and three phishing incidents of more than $100,000,000 lost. This represents nearly half of all value stolen in the year and **39.1%** of the number of incidents suggesting that, on average, phishing attacks typically lead to larger amounts stolen per incident than other vulnerabilities.
- Private key compromises followed, with **$855,385,570** stolen across **65** incidents. All four quarters of 2024 saw high levels of activity involving phishing attacks and private key theft.
- Ethereum experienced the highest number of security incidents, with a total of **403** hacks, scams, and exploits leading to **$748,688,677** in losses. This resulted in an average of **$1,857,788** stolen per incident.
- Hackers also frequently targeted Bitcoin and Tron, with **$542,700,000.00** and **$133,003,944.04** stolen, respectively.
- Security breaches affecting multiple chains accounted for **$435,045,134.22** in losses across **39** incidents.

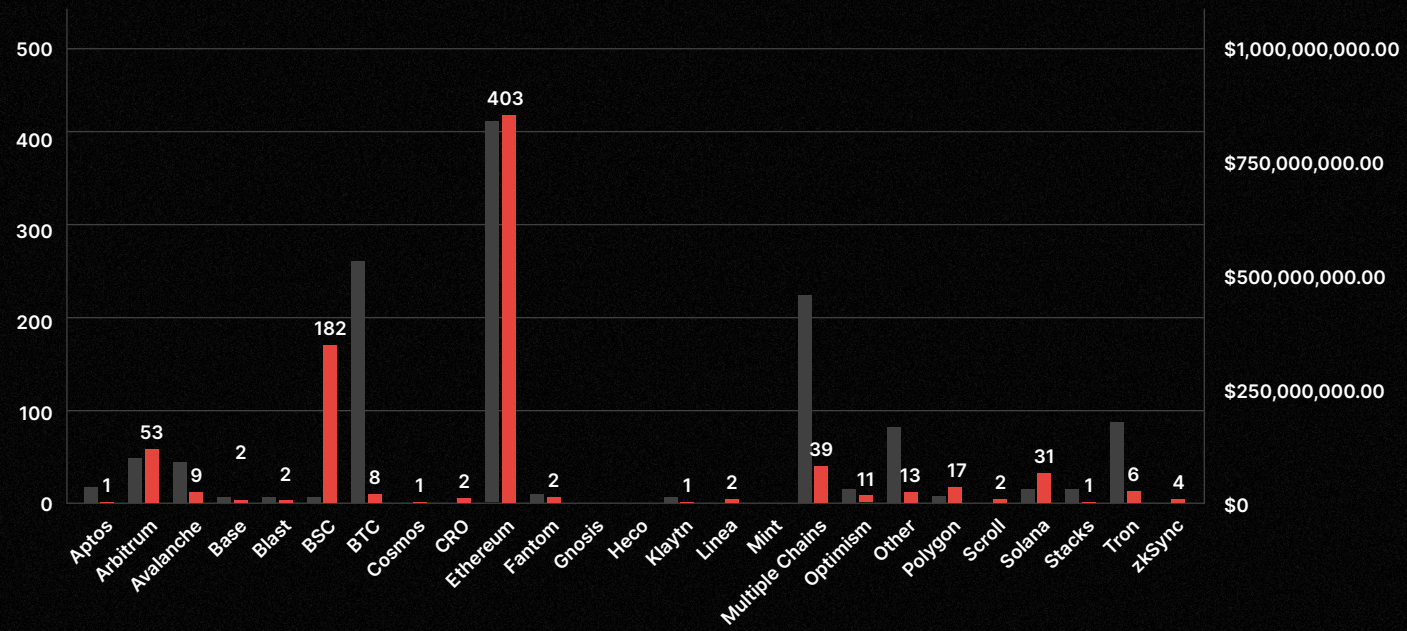
Hack3d 2024 covers the stories and trends that defined the direction of Web3, the current state of the industry, and where the next year might take us.

Statistics and Graphs: 2024 Year in Review

Incidents x Losses in 2024

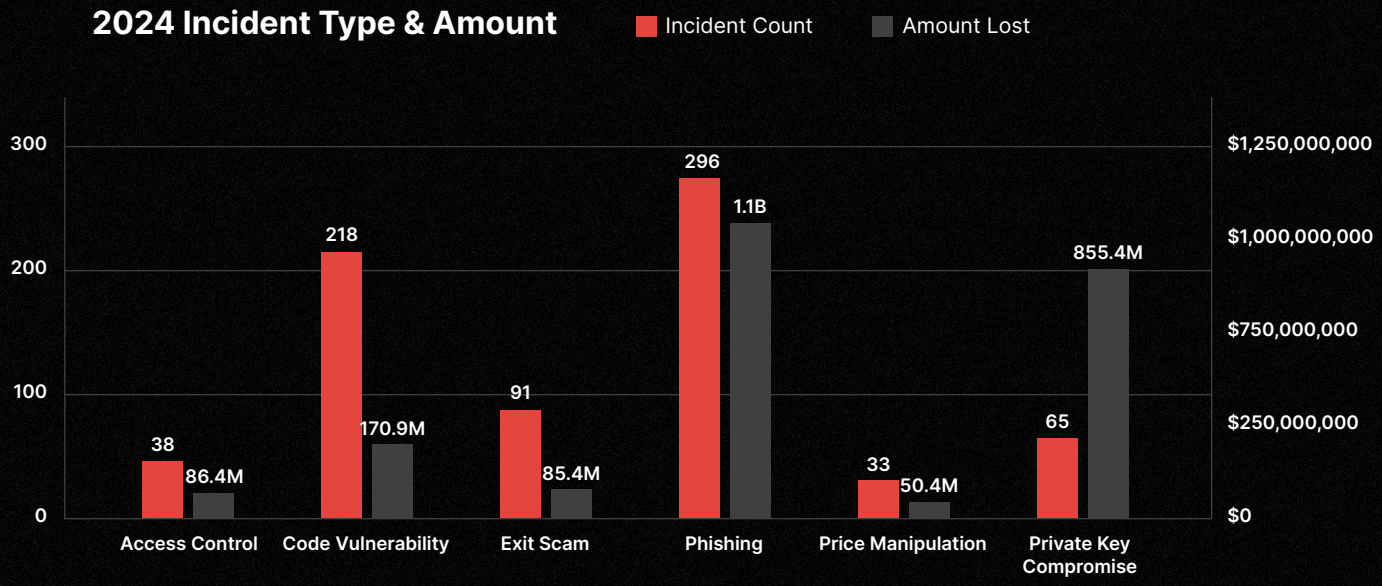


Incidents x Losses By Chain

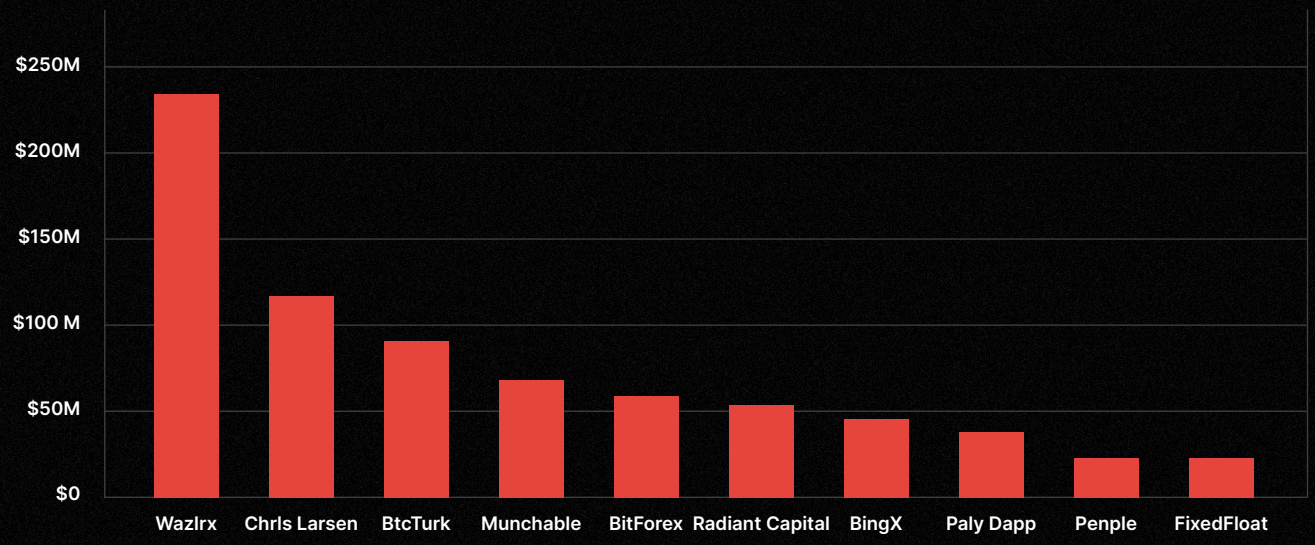


Statistics and Graphs: 2024 Year in Review

2024 Incident Type & Amount



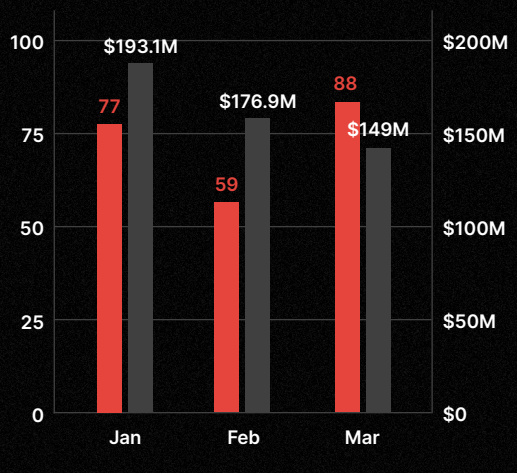
Top 10 Most Costly Incidents:



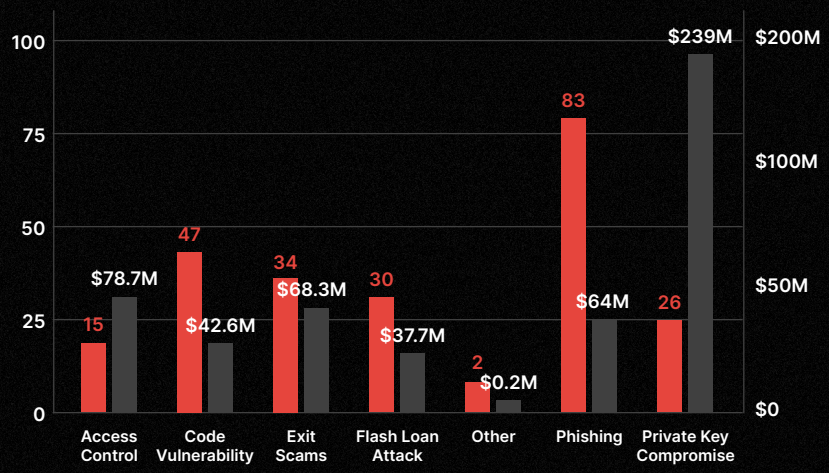
Statistics and Graphs: Q1 2024

Incident Count SAmount

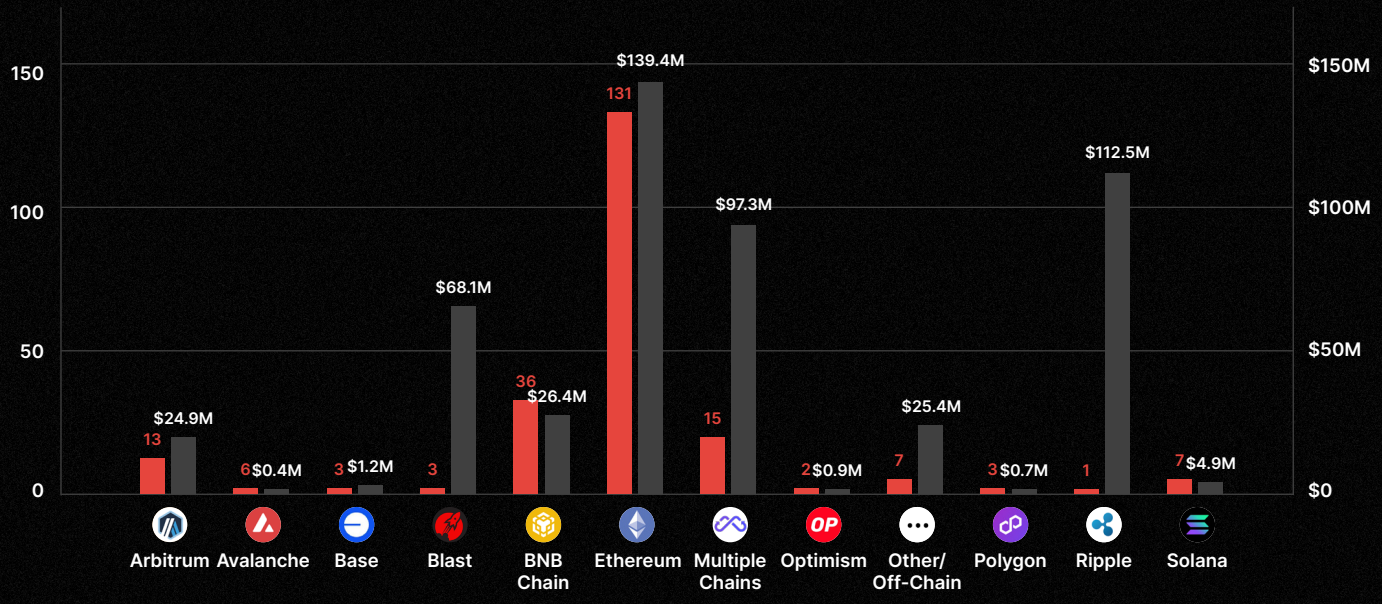
BY MONTH



BY TYBE



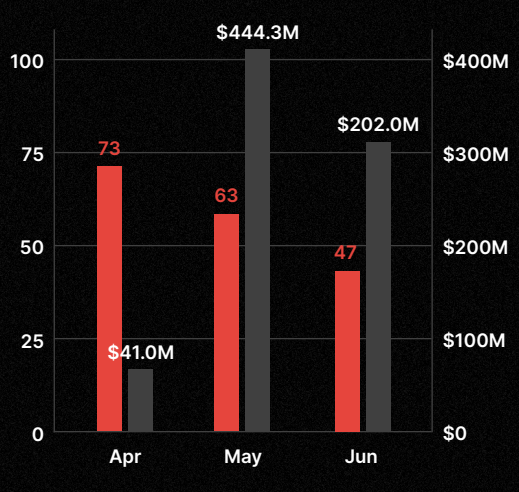
BY CHAIN



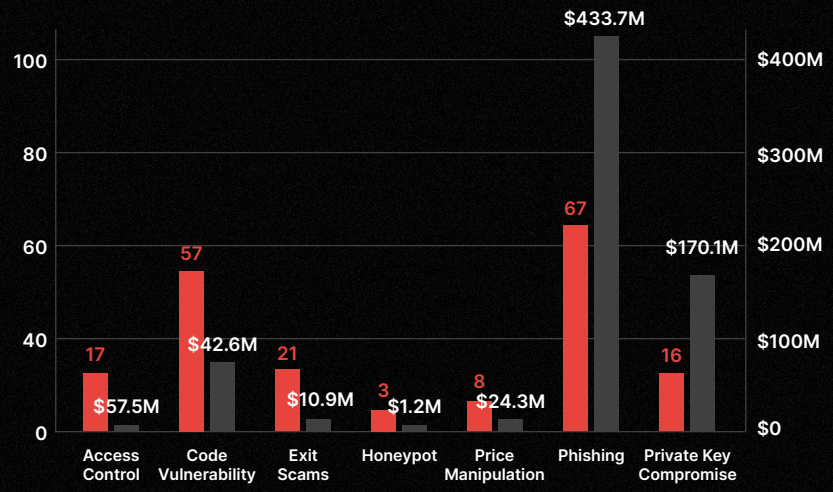
Statistics and Graphs: Q2 2024

Incident Count SAmount

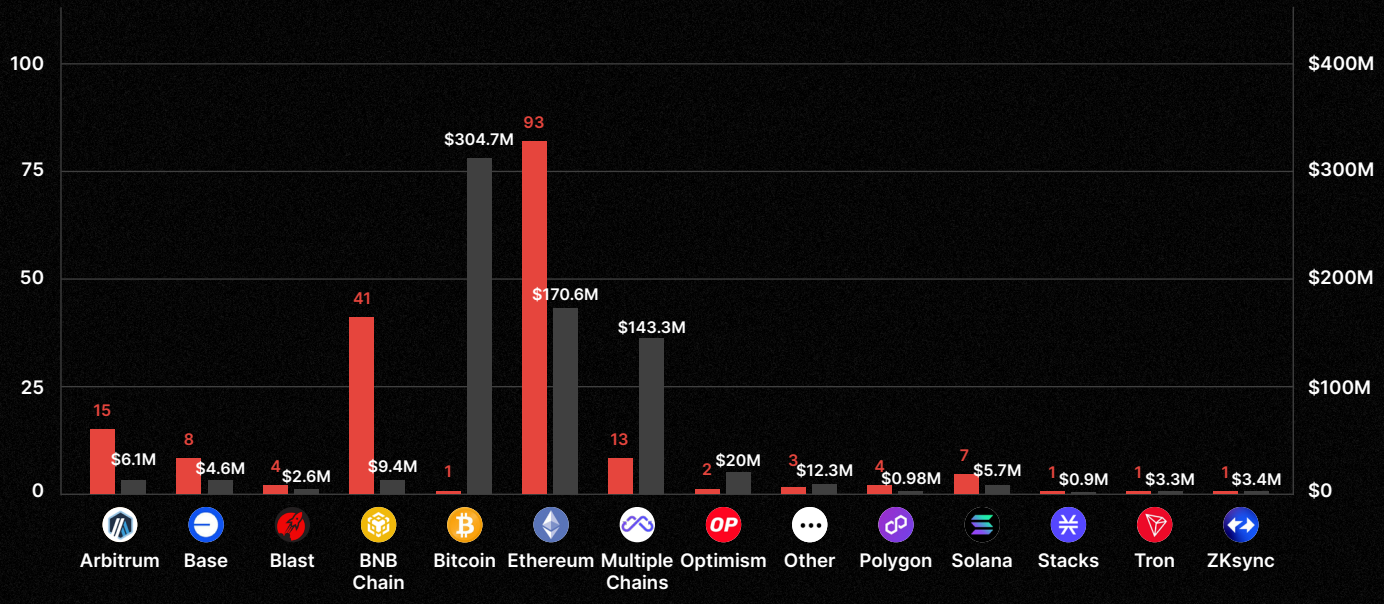
BY MONTH



BY TYBE

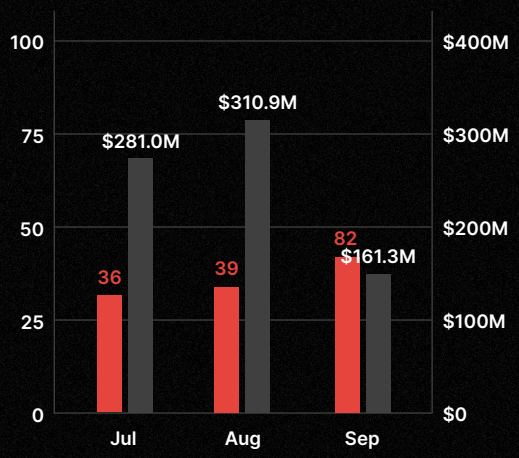


BY CHAIN

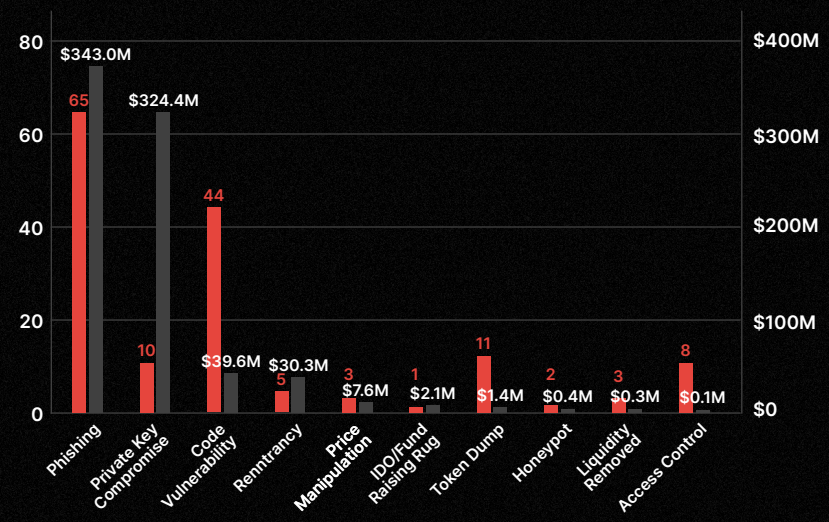


Statistics and Graphs: Q3 2024

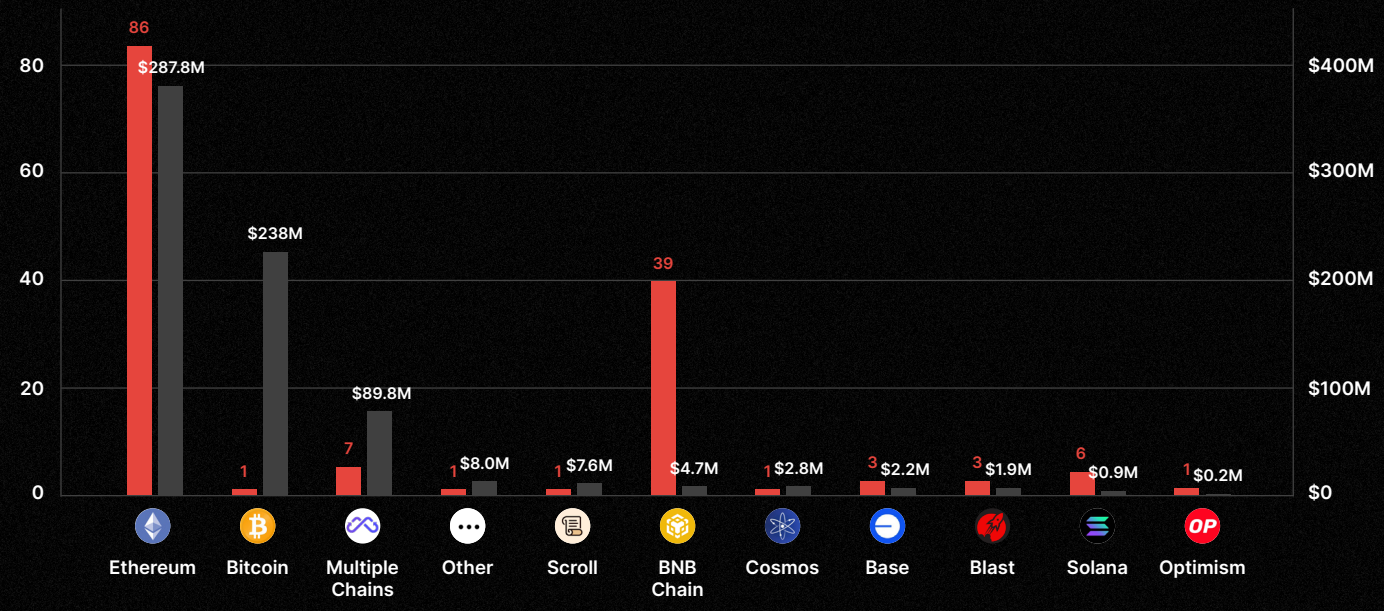
BY MONTH



BY TYBE



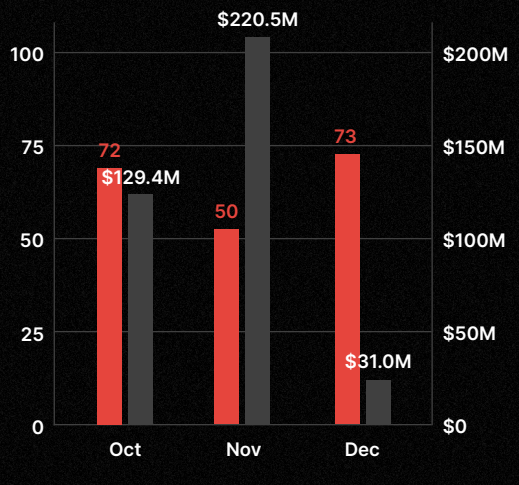
BY CHAIN



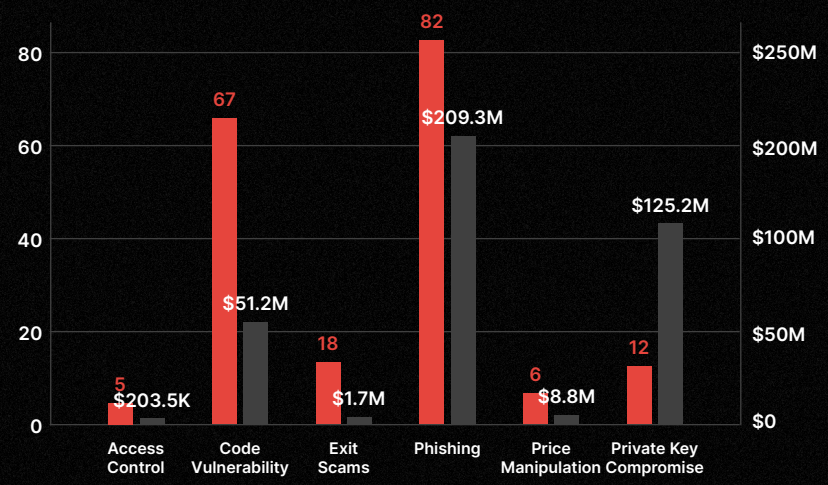
Statistics and Graphs: Q4 2024

Incident Count SAmount

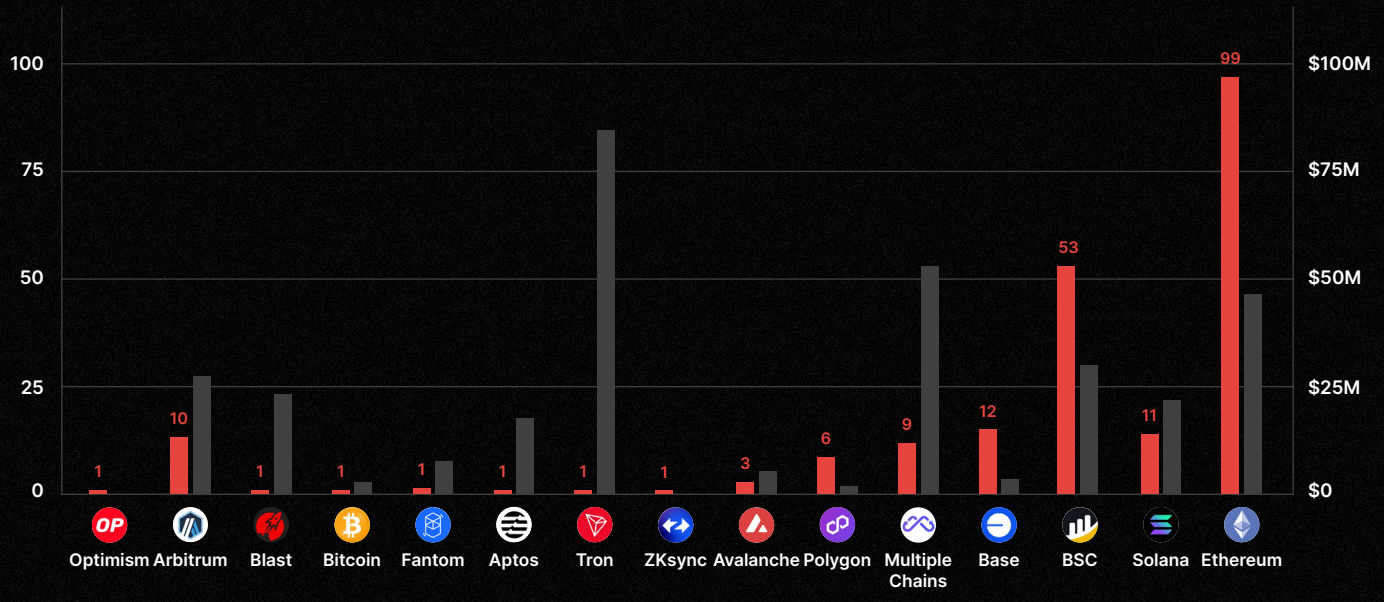
BY MONTH



BY TYBE



BY CHAIN

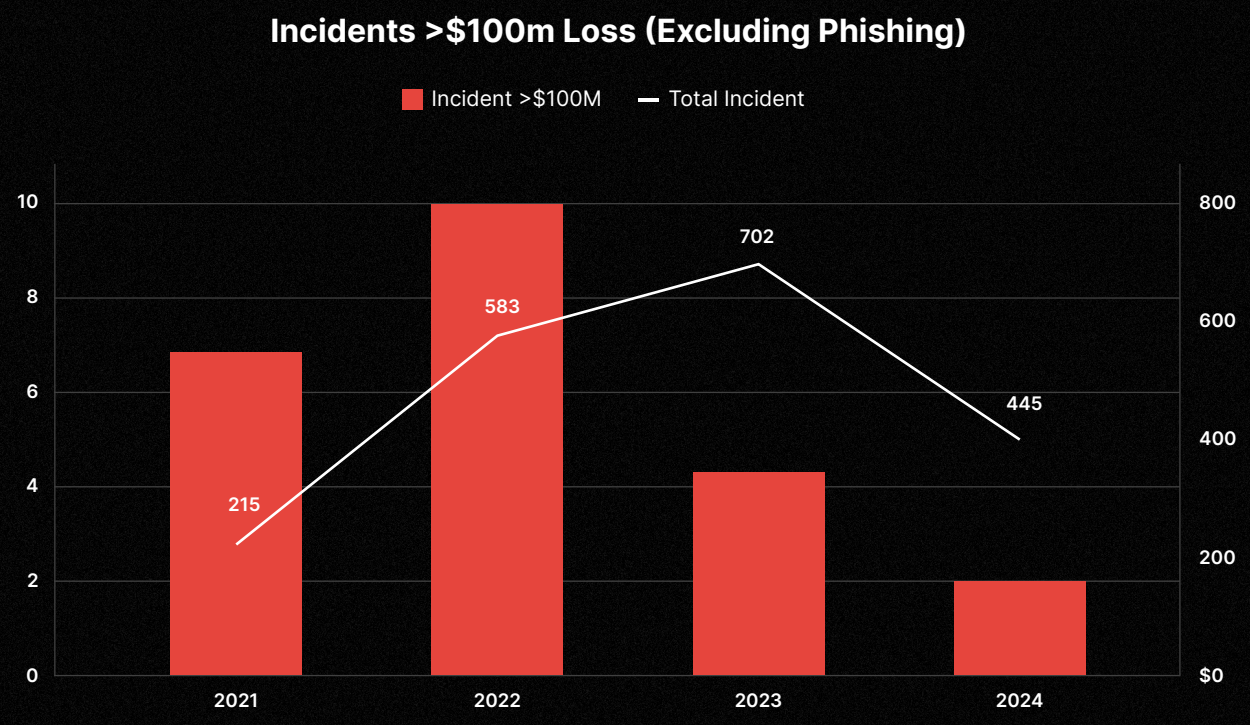


Overview

In 2024, the cryptocurrency industry experienced significant milestones, reflecting its growing acceptance and integration into mainstream finance. However, this expansion has also highlighted the critical importance of robust security measures to protect the increasing capital at stake.

Compared to 2023, the amount stolen in crypto-related incidents increased by approximately **31.61%** year-over-year, reaching a total of **$2,339,075,289.45** lost. This figure doesn't rival the $5,275,608,458.00 stolen in 2021, nor the $3,504,846,608.90 stolen in 2022; regardless, the overall increase from the prior year is still cause for concern.

It is important to note, however, that if we exclude phishing from the total, which represents nearly half of all value stolen this year, it seems that ecosystem security is getting better. For instance, in 2021, the top two incidents were the **$2.7 billion** Thodex exploit and the **$602 million** Poly Network exploit. In 2022, the top two exploits involved Ronin Network ($624 million lost) and FTX (**$477 million** lost). The only incident from 2024 to make it into the top 20 incidents since January of 2021 is WazirX at **$231 million**, suggesting that the number of incidents breaking $100 million in losses has come down.



2024 saw the cryptocurrency industry gaining further acceptance in traditional finance, marked by significant milestones that reshaped the market landscape. The approval of spot Bitcoin and Ethereum exchange-traded funds (ETFs) by the U.S. Securities and Exchange Commission (SEC) was among the most notable developments. After years of anticipation, the SEC greenlit 11 spot Bitcoin ETFs, including those from prominent firms like BlackRock and Fidelity. By July, Ethereum ETFs followed suit, offering institutional investors new opportunities to diversify their portfolios and signaling mainstream validation for these digital assets.

The steady recovery from the prolonged "crypto winter" continued throughout the year, as renewed institutional confidence brought a wave of investment back into the market. This steady influx laid the groundwork for Bitcoin's historic milestone of surpassing $100,000 in value, which occurred in the aftermath of the 2024 U.S. presidential election, and caused other popular cryptocurrencies to rise in tandem, such as Ethereum and Solana.

It is clear that the re-election of Donald Trump marked a turning point for the cryptocurrency industry in the U.S., which will likely influence other crypto markets around the world. Trump's administration quickly signaled a pro-crypto stance by appointing Paul Atkins, a prominent blockchain advocate, to lead the SEC. Elon Musk's appointment as head of the "Department of Government Efficiency" (DOGE) added momentum to the administration's pro-crypto agenda and drove a surge in Dogecoin's value.

Although we must wait until mid-January 2025 to see how these developments will actually play out, Trump has made additional crypto-related promises, including establishing a national Bitcoin reserve, stopping the creation of a U.S. central bank digital currency (CBDC), and supporting U.S.-based Bitcoin mining.

On the global front, additional regulatory developments in 2024 have showcased the diverse approaches governments are taking toward crypto adoption. For instance, the European Union advanced its Markets in Crypto-Assets regulation (MiCA), creating a unified crypto framework across member states. MiCA's requirements for transparency, liquidity, and consumer safeguards aim to foster innovation while ensuring crypto market integrity.

Asia presented a mix of regulatory strategies. Despite approvals in other markets, Japanese regulators have not endorsed crypto ETFs, citing concerns over investor protection and market stability. Additionally, Japan's Financial Services Agency (FSA) recently intensified its oversight by issuing warnings to unregistered overseas crypto exchanges operating without authorization. Other developments include South Korea's Act on the Protection of Virtual Asset Users (VAUPA) and Hong Kong's crypto tax break proposal.

While regulatory developments across the global shape the crypto industry in different ways, one constant remains: the critical importance of security. As markets evolve and integrate into traditional financial systems, the risks associated with non-compliance, fraud, and theft continue to grow.

As a leader in crypto security, CertiK's mission is to help fortify the Web3 ecosystem, utilizing industry-leading formal verification technology to protect and monitor blockchain protocols and smart contracts. We apply cutting-edge innovations from academia to enterprise, enabling mission-critical applications to scale with safety and correctness. To date, we have worked with more than 4,800 enterprise clients, secured more than $511 billion worth of digital assets, and detected more than 115,000 vulnerabilities in blockchain code.

Our mission is ongoing, and 2024 has seen achievements like being acknowledged by Apple for the sixth time for identifying a vulnerability in Apple Vision Pro's eye tracking technology, and being recognized by Samsung for the third time for discovering a high-severity vulnerability in the Blockchain Keystore. We completed formal verification of the ZKWasm Circuit consisting of 144 instructions, marking the first complete formal verification effort within the zero-knowledge proof ecosystem. Another notable achievement involved extending our research into the Decentralized Physical Infrastructure Network (DePIN) space, helping projects like APhone and Aethir mitigate security risks. And finally, we audited six of Forbes' top 10 tokens in the first half of 2024, which includes TON, Core DAO, PEPE, FLOKI, FET, and Bitget.

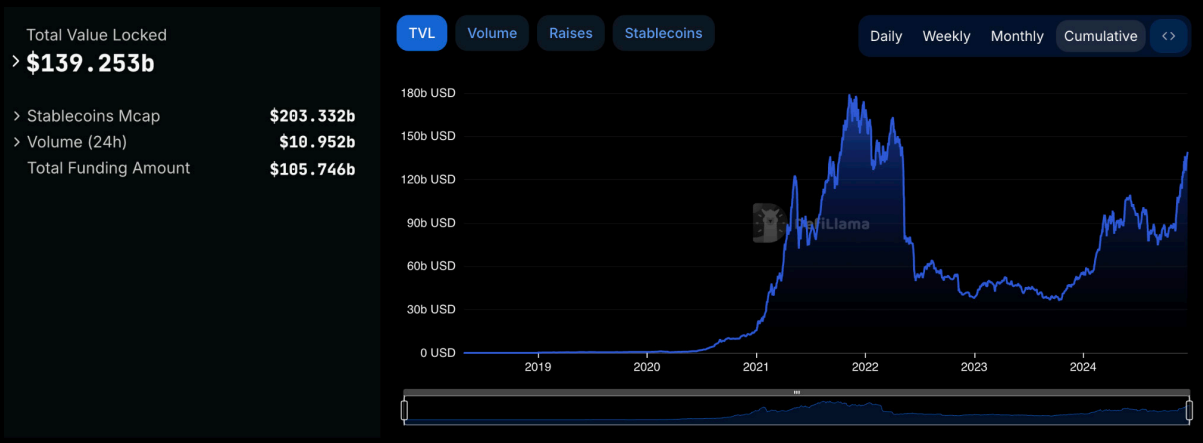
On the regulatory front, we provided two stablecoin proposals to the Hong Kong Monetary Authority (HKMA) and Hong Kong's Financial Services and the Treasury Bureau (FSTB), both of which were approved.

Although the crypto industry is progressing in exciting ways, we recognize that the decentralized future hinges on trust. Without robust security and regulatory alignment, crypto participants will continue to encounter risks — we only have to look at the fact that malicious actors stole more than **$2.3 billion** in 2024.

In our Hack3d reports, we aim to examine the industry's vulnerabilities in greater detail and assess its resilience. First, we look at a statistical analysis of 2024's figures, including the most commonly used attack vectors, most exploited chains, and how amounts stolen fare against factors like total value locked (TVL). We also explore the top incidents of 2024, other notable industry developments, and best security practices for crypto participants.

Funds Stolen in Perspective: Measuring Risk Amid Rising TVL

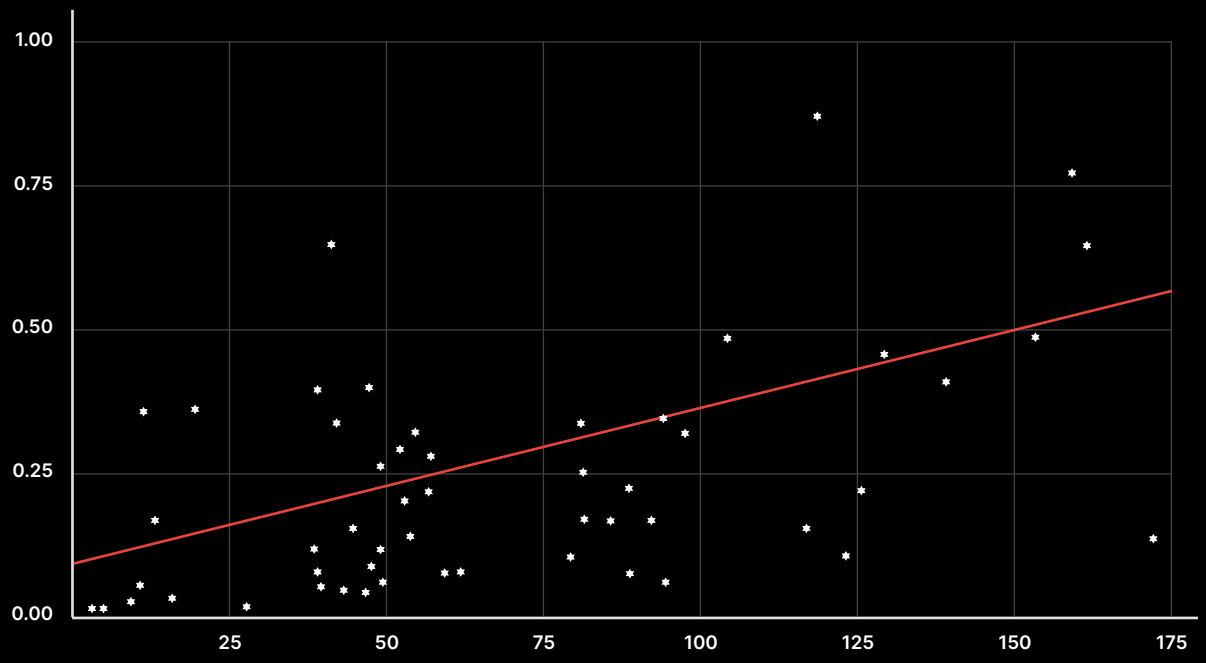
In 2024, total value locked (TVL) across blockchain networks increased substantially, with Ethereum liquid staking alone surging from approximately $248 million in January 2024 to $17 billion in December 2024. This increase, which began toward the end of 2023, highlights the renewed adoption of DeFi 2024.



Source: DeFiLlama

TVL reflects the total amount of assets actively staked, pooled, or locked in decentralized protocols. It is a critical indicator of the adoption and trust in blockchain technology, providing insight into the financial health and scale of the ecosystem. A rising TVL can signal growing confidence from users and institutions, while fluctuations can point to shifts in activity or concerns about risk. By examining the amount of stolen funds in the context of rising TVL, we can better understand the effectiveness of security measures relative to the sector's growth.

The following scatter plot charts the correlation between monthly losses to hacks and scams in 2024, and TVL in DeFi. TVL values are taken on the last day of each month from DeFiLlama's dataset, and value lost due to hacks and scams are monthly totals from our own data.



There is a moderate positive correlation between TVL and monthly losses, with an R2 value of 0.32. This suggests that approximately 32% variability in monthly losses can be statistically attributed to changes in DeFi's TVL. The trend line's uptrend indicates that, as TVL increases, there is a tendency for losses from security incidents to rise in tandem—but this isn't in a strictly proportionate manner. Although this correlation is statistically significant, it leaves 68% of the variability unexplained by just TVL; consequently, it is clear that other factors play a role in influencing losses. Here are some of those factors:

- **Evolving Attack Techniques:**

  Hackers are constantly refining their methods, employing advanced tactics like social engineering and zero-day exploits, which target vulnerabilities beyond basic security measures.
- **Variable Security Standards:**

  Differences in the quality of security across projects and exchanges can significantly impact losses. Protocols with inadequate audits, weak smart contract designs, or poor private key management are more susceptible to attacks.
- **Regulatory Gaps:**

  Inconsistent regulations across jurisdictions can affect the prevalence of theft. For instance, stricter regulatory environments may deter such activities in some cases.
- **Market Conditions:**

  High-value markets or price spikes may increase the rewards for successful attacks, incentivizing more hackers to act.
- **Protocol Complexity:**

  More intricate DeFi protocols can introduce hidden vulnerabilities that attackers exploit. These technical flaws can arise from the challenges of balancing innovation with thorough security testing.

- **Centralized Weak Points:**

  Centralized systems create concentrated risks; compromising these points can lead to disproportionately large losses unrelated to the decentralized TVL.

2024's R2 value of 0.32 is only a slight increase from 2023's value of 0.31. This minimal difference, despite the substantial growth in TVL in 2024, offers an intriguing insight into the evolving dynamics of the ecosystem. In addition to the other relevant factors mentioned above, it is possible that the amount stolen isn't scaling proportionally with TVL. This could indicate that improved security measures, greater awareness, and more robust defenses are mitigating some of the risks typically associated with higher levels of TVL. While this is an encouraging sign, it also underscores the need to continue addressing vulnerabilities and monitoring other factors that may influence losses as the industry grows.

Phishing:
2024's Leading Cyber Threat

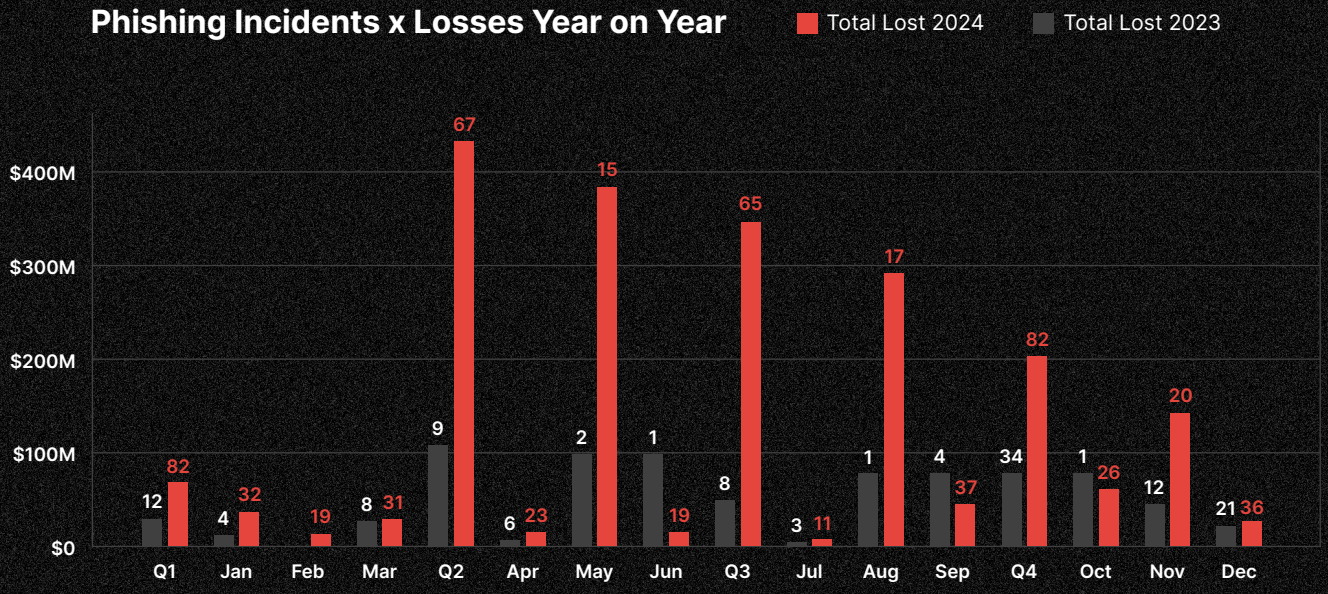
Phishing was the most costly attack vector in 2024, with a total of **$1,050,129,497.68** lost across **296** incidents. These figures represent nearly half of all value stolen in the year and **39%** of the total number of incidents, suggesting that, on average, phishing attacks typically lead to larger amounts stolen per incident than other vulnerabilities.

The average amount lost per attack is **$2,827,033** and the median amount lost is **$207,556**. Hackers returned **$213,327,829**, placing adjusted losses at **$836,801,668**.

Phishing's popularity among attackers stems from its simplicity and effectiveness: Phishing preys on human vulnerabilities rather than solely targeting technological defenses. By crafting deceptive emails, fake websites, or fraudulent messages, attackers trick users into divulging sensitive information like passwords, private keys, or wallet addresses. In the crypto space, the irreversible nature of transactions makes phishing particularly devastating, as funds cannot be recovered once transferred—unless the attacker decides to return funds.

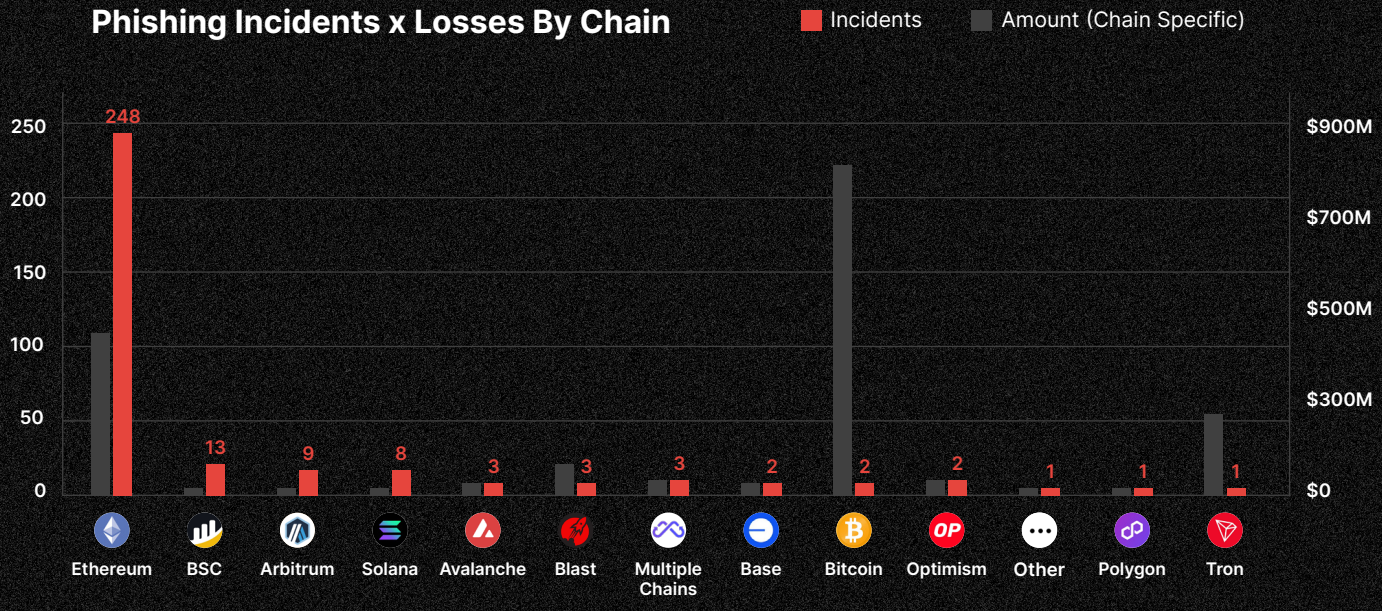
In terms of quarterly losses due to phishing attacks, Q2 is the largest in 2024, with **$433,688,871** stolen across **67** incidents. Since then, the amount lost has been on a steady decline. Regardless, 2024's figures are substantially higher than those of 2023; for example, Q2 of 2023 saw **$103,157,766** lost due to phishing attacks, which is lower than three of the four quarters in 2024.

Phishing Incidents x Losses Year on Year



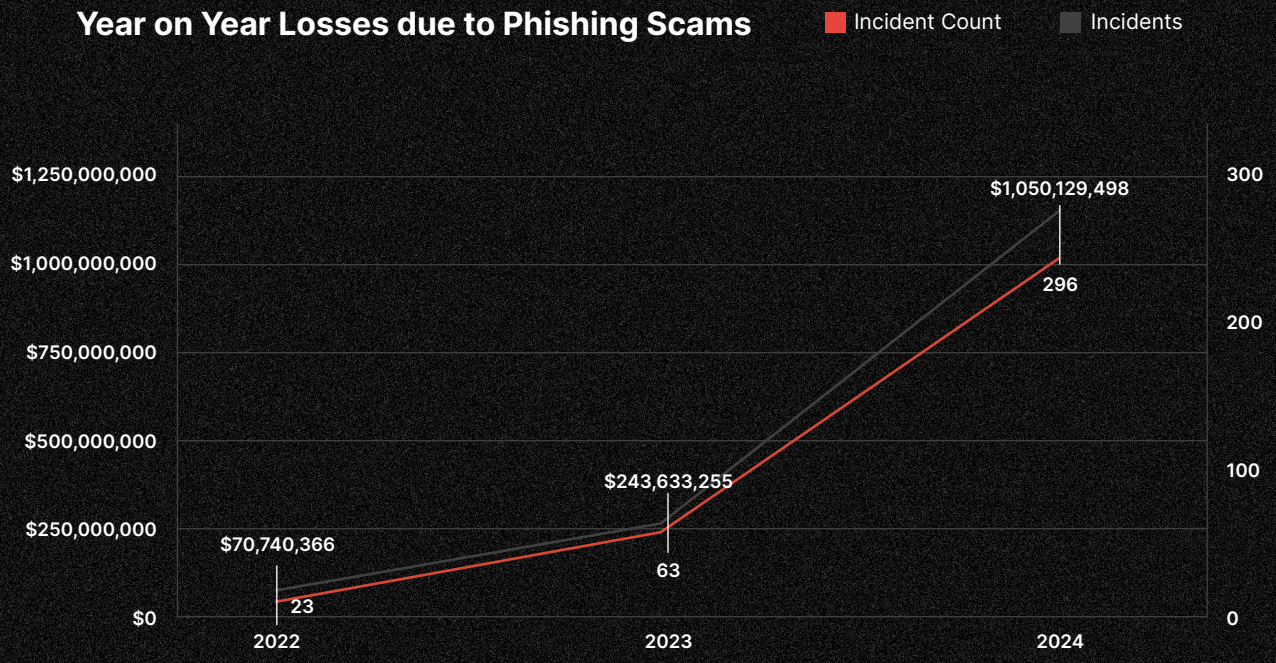
Given that Ethereum was the most targeted chain across all attack vectors, it is no surprise that this is also the case for phishing. **$297,522,298.3** was stolen on Ethereum across **248** incidents. Binance Smart Chain (BSC) was another common target for phishing attacks.

Phishing Incidents x Losses By Chain



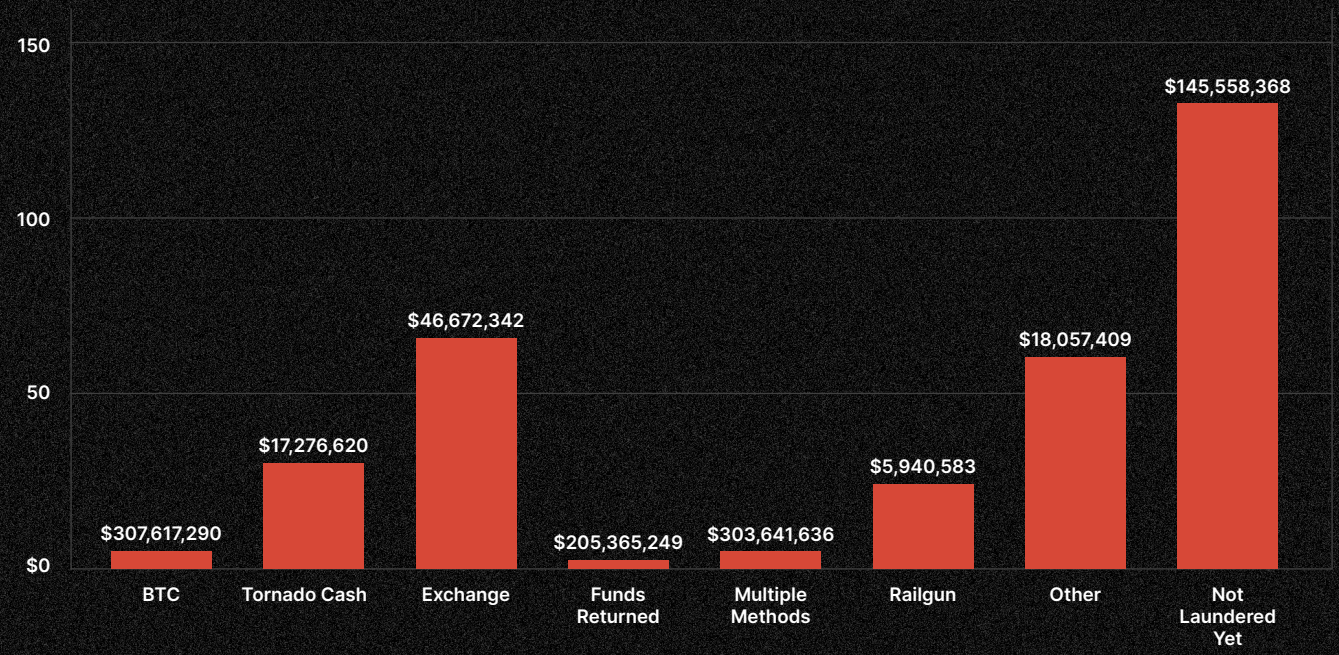
Year on year losses due to phishing scams are also increasing at a rapid pace. Between 2022 and 2023, phishing losses increased by 244.41%. Between 2023 and 2024, losses increased by **328.61%**.

Year on Year Losses due to Phishing Scams



After successful phishing attacks, hackers often engage in laundering methods in an attempt to make the stolen funds harder to trace and recover. However, it appears that the majority of funds stolen due to phishing attacks have not yet been laundered. Other popular methods include using centralized exchanges and Tornado Cash.

Laundering Method



How to Protect Yourself Against Phishing

- **Be Skeptical of Unsolicited Communications:**

  Exercise caution with unexpected emails, messages or calls—especially those requesting personal information or urging immediate action. Verify the sender's authenticity through official channels before responding.
- **Examine Email and URL Details:**

  Scrutinize email addresses and website URLs for subtle misspellings or unusual characteristics that may indicate fraudulent sources. Hover over links to preview URLs without clicking to see if they direct to legitimate sites.
- **Enable Two-Factor Authentication (2FA):**

  Implementing 2FA adds an extra layer of security by requiring a second form of verification, such as a unique code sent to your device, reducing the risk of unauthorized access.
- **Keep Software Updated:**

  Regularly update your operating systems, browsers, and applications to patch vulnerabilities that cybercriminals could exploit, whether through phishing or other forms of attacks.
- **Continuously Educate Yourself:**

  Stay informed about the latest phishing tactics and scams. Participate in cybersecurity training at your organization and regularly review resources to recognize and avoid potential threats.
- **Verify Wallet Addresses:**

  Always double-check wallet addresses before sending crypto. Hackers can use phishing tactics to swap legitimate addresses with fraudulent ones, leading to irreversible loss of funds.
- **Use a Hardware Wallet:**

  Storing your cryptocurrency offline protects it from phishing attacks that target online wallets or exchanges.
- **Avoid Public Wi-Fi for Transactions:**

  When accessing your wallet or making transactions, use a secure and private internet connection. Public Wi-Fi can expose you to phishing attacks and man-in-the-middle threats.

Additional Reading

Trap Phishing on Trusted Platforms: A New Phishing Trend in The Web3 World

In this blog, we discuss a new form of active phishing within the Web3 ecosystem, which involves deploying phishing traps on influential platforms like exchanges and marketplaces to enhance the outreach and credibility of the phishing sites. These traps take various forms, such as deceptive Web3 project job ads, enticing airdrops, and fabricated NFT sales from counterfeit project sites.

Modal Phishing in Web3 Mobile Wallets

We discuss a phishing technique, Modal Phishing, which is often to mislead victims about the identity of connected dApps. Attackers can send crafted messages to mobile wallets, impersonating a legitimate dApp and tricking victims into approving transactions by showing misleading information in the modal of mobile wallets.

Ice Phishing Scams

A type of phishing unique to the Web3 space, known as ice phishing, is a significant threat to the community. Instead of acquiring users' private keys and seed phrases, scammers trick victims into approving the transfer of assets to the scammer's wallet. This method has been used to steal users' tokens and NFTs worth millions of dollars.

What Is a Phishing Attack? Tips on How to Protect Yourself

In this blog, we discuss the different types of phishing attacks, including fake browser extensions, fake apps, and DNS hijacking. We also explore real-world examples of phishing and tips on how to protect yourself from these types of scams.

DMM Bitcoin Incident Analysis

On May 31, 2024, Japanese exchange DMM Bitcoin released a statement, saying that **4,502.9** BTC, worth approximately **$304** million at the time, was withdrawn from their wallet without authorization.

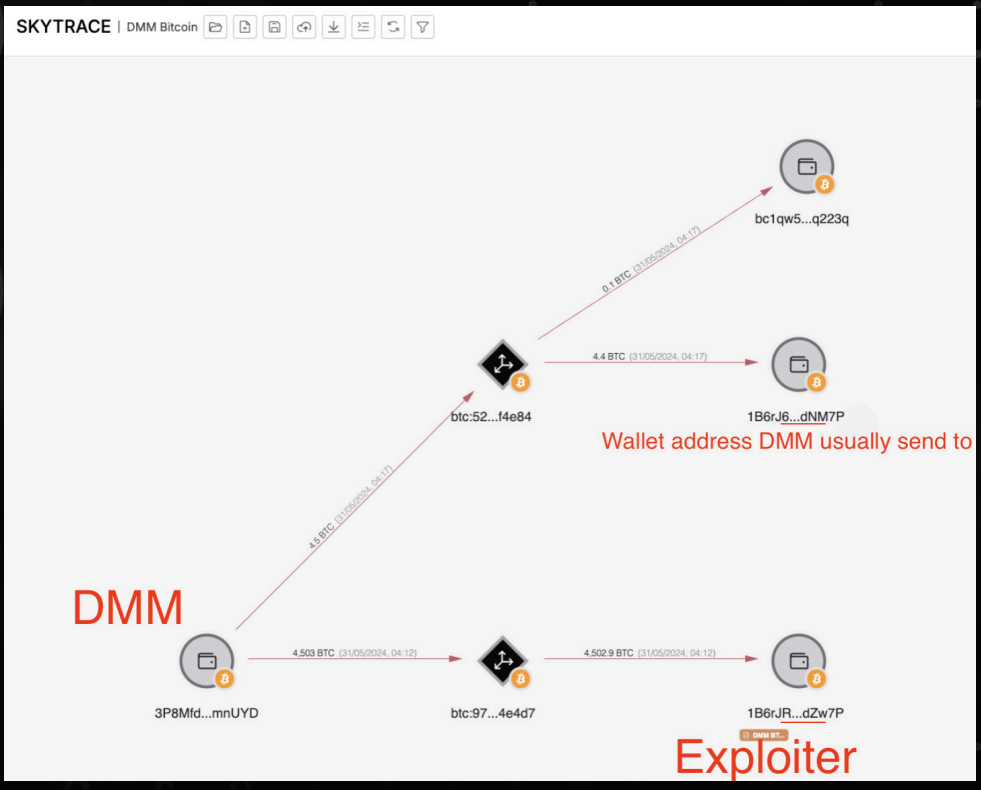
The loss was likely the result of address poisoning, a phishing method by which a wallet with a similar address to one used by a victim inserts itself into its transaction history, thereby "poisoning" it. The wallet will usually have the same start and ending characters as one used by the victim, in the hope that an unsuspecting user will copy the wrong address. Prior to the BTC being sent to an unauthorized wallet, the unauthorized wallet had initiated a transaction to the DMM wallet.

Although the source of the attack is unclear, several media outlets and industry experts have speculated that North Korean hacker group, Lazarus Group, was involved.

Using the SkyTrace feature of CertiK's SkyInsights, we can see that **4,502.9** BTC moved from DMM to the exploiter's address. We can also see the similarities between the exploiter's wallet address and the one DMM usually sent funds to.

Exploiter Transaction:

https://bitaps.com/975ec405ac9dc9fa5ab8009d94d6a1fe31dff8a8127ea90d023104e52754e4d7



In December 2024, DMM Bitcoin announced that it would be shutting down operations after making a deal to transfer its remaining assets to trading platform SBI VC Trade. DMM Bitcoin stated, “We have determined that allowing this situation to continue for a long time would significantly impair customer convenience.In light of this situation, and with the protection of our customers as our number one priority, we have decided to transfer all accounts and assets held with us to another company. We sincerely apologize for the inconvenience caused to you over such a long period of time. As a result, the Company plans to discontinue its business once the transfer is complete.”

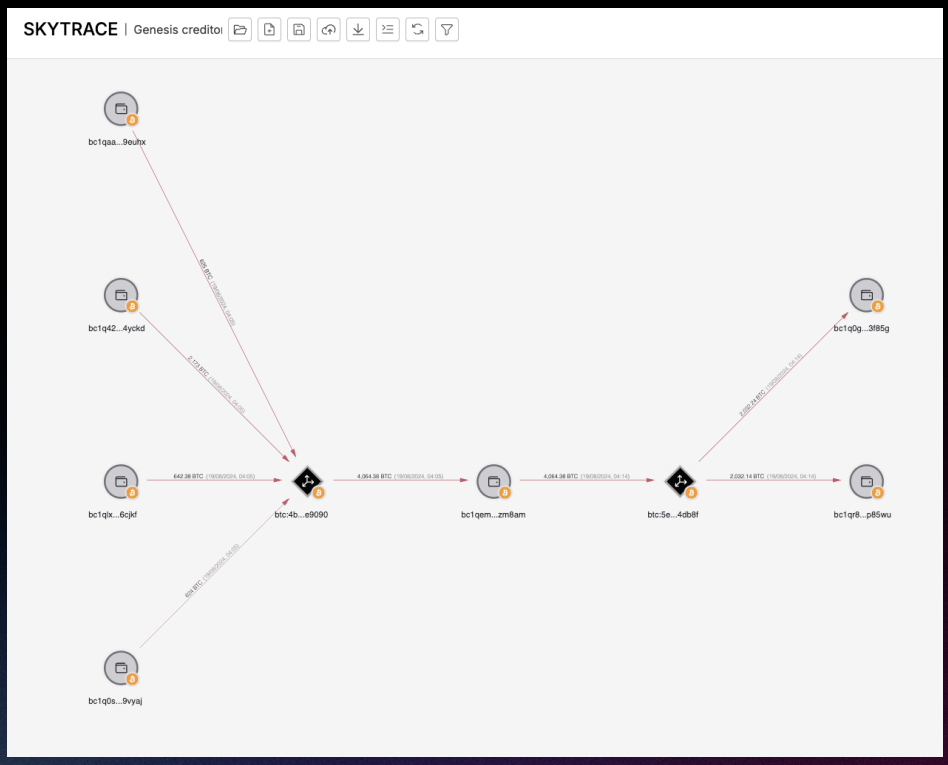
Other Notable Incidents

The methods employed by cybercriminals to steal crypto are as varied as they are effective. From highly targeted social engineering schemes to more technical exploits like address poisoning, bad actors continuously innovate to compromise security and evade detection. The following three incidents underscore the range of tactics used to steal digital assets and highlight the importance of staying vigilant.

$243 Million Stolen in Social Engineering Attack

In August 2024, a sophisticated social engineering attack led to the theft of $243 million in crypto from a single Genesis creditor located in Washington, D.C. The attackers, who posed as support employees from Google and Gemini, tricked the victim into resetting their two-factor authentication (2FA) and transferring funds to a compromised wallet. Using remote access software AnyDesk, they further exploited the victim to extract private keys stored in a Bitcoin Core wallet.

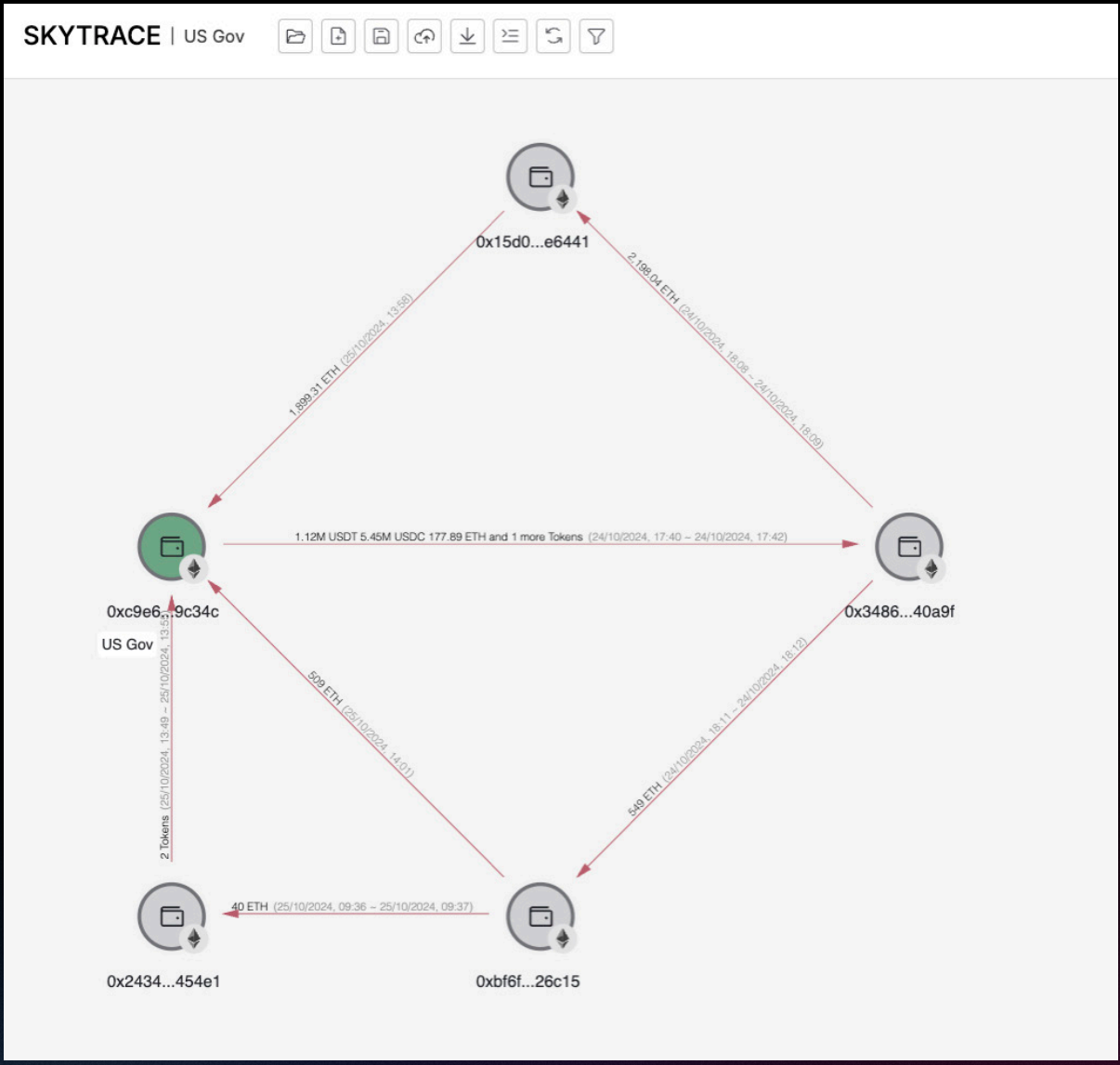
Crypto investigator ZachXBT played a pivotal role in the aftermath of this exploit, tracing the movement of the stolen Bitcoin using transaction hashes. His findings led to the identification and arrest of suspects who were charged with conspiracy to steal and launder crypto. The Department of Justice confirmed that millions in stolen funds were recovered, marking a major breakthrough in tackling large-scale crypto theft.



Compromised Wallet Likely Owned by U.S. Government

On October 24, 2024, a hacker compromised a wallet likely controlled by the U.S. government, draining $20 million in funds previously seized from the 2016 Bitfinex hack. After gaining unauthorized access, the attacker transferred the stolen funds, including stablecoins such as USDC and USDT, to a wallet they controlled. Then they began converting the stablecoins into Ether and laundering the assets through addresses suspected to be tied to a money laundering platform.

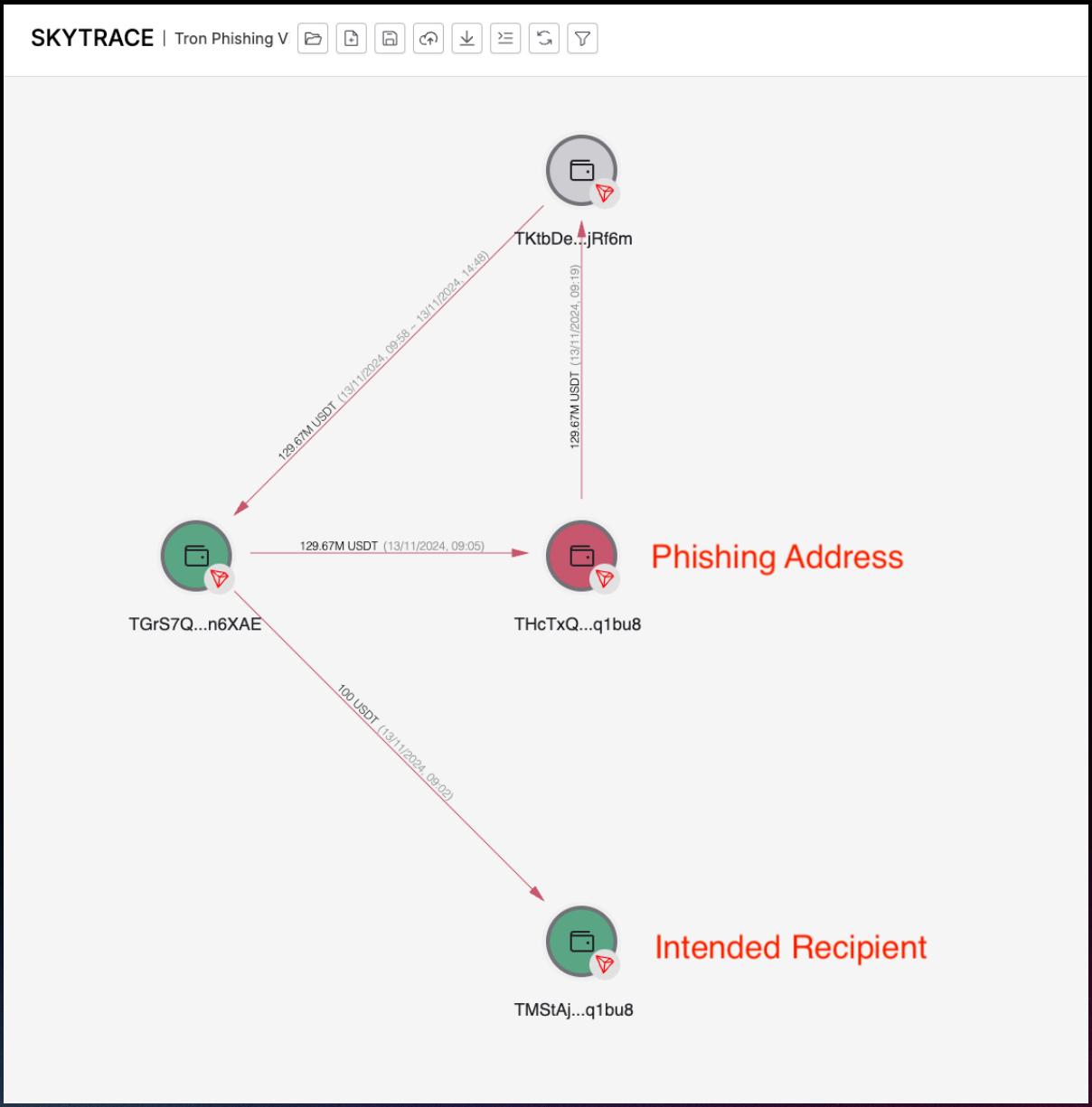
The incident occurred just weeks before the sentencing of Ilya Lichtenstein and Heather Morgan, the Bitfinex exploiters, reigniting concerns over the long-term security of seized digital assets. Despite the U.S. government's success in recovering some Bitfinex funds in the past, this hack illustrates the risks in safeguarding crypto assets—particularly those associated with high-profile cases.



$129 Million Address Poisoning Victim

On November 20, 2024, a crypto user fell victim to an address poisoning scam, resulting in the temporary loss of $129 million. The scammer infiltrated the victim's transaction history by sending small, seemingly legitimate transactions to their wallet, ensuring the scammer's address appeared as a trusted contact. When the user attempted a large transfer, they inadvertently copied and sent funds to the scammer's wallet.

Remarkably, the scammer returned the full amount within an hour. While the exact reason for this remains unknown, it is speculated that the scale of theft may have prompted fears of legal repercussions or significant attention from the crypto community. The quick restitution, however, does not diminish the lessons this case offers about the importance of manually verifying wallet addresses before initiating transactions.



2024 at CertiK

2024 was a big year at CertiK. Here are some of our notable achievements this year:

- Advised the Monetary Authority of Singapore (MAS) on its stablecoin frameworks, earning recognition.
- Uncovered a significant vulnerability in CosmWasm, which allowed untrusted Wasm submissions across more than 20 App Chains within the Cosmos ecosystem.
- Acknowledged by ByteDance for identifying and mitigating a substantial security risk within the systems of ByteDance, the creator of TikTok.
- Identified a vulnerability risk within Ant Group and reported it to the AntSRC, which led to the swift and successful implementation of the necessary security measures.
- Completed formal verification of the ZKWasm Circuit consisting of 144 instructions, marking the first complete formal verification effort within the zero-knowledge proof ecosystem.
- Conducted rigorous penetration testing on Bybit's Keyless Wellets, a crucial component serving more than 1 million users.
- Conducted a security assessment of the first public SDK for GalaChain, and carried out performance testing of GalaChain using the SDK, uncovering several system-level efficiency issues that helped their team enhance the codebase.
- Refined our brand with a new customer-centric slogan, "Elevating Your Entire Web3 Journey," emphasizing our commitment to a complete range of innovative, full-cycle products and services.
- Ranked first on TON's official list of Security Assurance Providers.
- Received sixth acknowledgement from Apple for identifying a vulnerability in Apple Vision Pro's eye tracking technology.
- Provided two stablecoin regulatory proposals to the Hong Kong Monetary Authority (HKMA) and Hong Kong's Financial Services and the Treasury Bureau (FSTB), both of which were approved.
- Audited six of Forbes' top 10 tokens in the first half of 2024, which includes TON, Core DAO, PEPE, FLOKI, FET, and Bitget.
- Extended our research into the Decentralized Physical Infrastructure Network (DePIN) space, helping projects like APhone and Aethir mitigate security risks. We shared insights from our DePIN experience at the 2024 Qualcomm Product Security Summit.
- Held nearly 50% of the global Web3 auditing market in July 2024.
- Recognized by Samsung for the third time for discovering a high-severity vulnerability in the Blockchain Keystore.
- Our CEO and Co-Founder, Professor Ronghui Gu, attended the 2024 Singapore FinTech Festival, and participated in interviews with major international media outlets, including Money FM, Lianhe Zaobao, Ming Pao, Hong Kong Economic Journal, and Bloomberg Businessweek.
- Ronghui Gu participated in a Fireside chat with CZ, where they discussed Web3 security challenges, blockchain innovation, and key questions shaping the future of the ecosystem.

CertiK's Security Suite

As part of our mission to secure the Web3 world, CertiK provides a number of tools designed to help projects and investors take an end-to-end approach to security.

CertiK KYC provides comprehensive and private identity verification for project teams. This process includes an ID authenticity inspection using AI-based detection systems, as well as liveness checks to ensure the individual is indeed real and matches the ID. CertiK will also undertake a live video call with each team member to verify their identity and other parameters as needed. As team anonymity increasingly enables high-risk behaviors, CertiK KYC helps to build accountability around projects to enable investors to move forward in trust. Projects that earn a Bronze, Silver, or Gold KYC Badge demonstrate to their community that they are willing to stand behind their project, sending a powerful message that they can be trusted to carry out the project's mission.

Penetration Testing is the final component of a comprehensive approach to securing crypto applications in a runtime environment. Our penetration testing services uncover even the smallest weaknesses by leveraging proprietary tooling, powered by an experienced team of ethical hackers.

CertiK Bug Bounty Program crowdsources intelligence from the world's top ethical hackers to uncover vulnerabilities before malicious actors can exploit them. CertiK's expert security engineers screen and qualify submissions and work with clients to implement the right fixes. Our 0% fee model reduces the payout pressure for projects and allows white hat hackers to receive the full bounty.

Get the most out of Web3 by partnering with **CertiK Advisory**. Our team of seasoned analysts deliver a comprehensive range of services, including technical evaluations, proprietary research, and strategy recommendations.

CertiK Security Score Leaderboard lists and ranks projects according to their Security Score. The Security Score is generated using a proprietary algorithm that takes into account a project's Code Security, Fundamental Health, Operational Resilience, Community Trust, Market Stability, and Governance Strength.

The Verified Teams Leaderboard lists and ranks projects based on the status of their CertiK KYC Badge. Project teams that successfully undergo a rigorous background investigation are granted the CertiK KYC Badge, which comes in Gold, Silver, and Bronze.

The Influencer Score Leaderboard lists and ranks Web3 influencers based on their influence score, which reflects the impact and reach of their content and online presence. This leaderboard is helpful for users who are interested in identifying influencers who are shaping the conversation in Web3.

Exchange Audit allows users to conduct due diligence on centralized exchanges (CEXs) by displaying the on-chain asset holdings in the wallet addresses controlled by the exchanges. This is an important first step for proof-of-reserve verification.

Skynet Alerts is a system that provides timely notifications on rugpulls and exploits in the cryptocurrency space. Skynet Alerts constantly monitors various sources of information to identify and report on potential rugpulls and exploits as they happen.

Smart Money Wizard is the access point for the Wallet Analyzer feature, and enables users to directly search for wallet addresses, view trending wallet searches, top smart money wallets, and top liquidity pairs. The Wallet Analyzer feature provides insights on wallet addresses and makes it easy to decipher on-chain transactions between wallets by displaying key wallet characteristics, visualizing wallet relationships and token trading activity.

Check out Skynet for Community platform today, read more on the Skynet education hub, and watch the masterclass on using Skynet to level up your due diligence research.

SkyInsights is a comprehensive crypto compliance and risk management platform. It offers wallet screening, real-time transaction monitoring, risk scores, and customizable alerts to help financial institutions, small-to-medium firms, and crypto-native platforms manage compliance complexities effectively. SkyInsights helps crypto-exposed organizations navigate regulatory landscapes efficiently while maintaining efficient processes and enhancing client trust.

Drawing from our experience in Web3 security, **CertiK SkyNode Service** provides a reliable and secure platform for hosting blockchain infrastructure. It offers a range of features, including node maintenance, an insightful performance dashboard, penetration testing, and resilient disaster recovery. Currently, more than six blockchain validator nodes, including BNB, exSat, Kaia, Keep, XRP sidechain, and Wemix, are hosted on the SkyNode platform.

Supported Ecosystems: CertiK's security services are available for all projects on all blockchains. A list of ecosystems we've worked with includes: