The Bybit Ethereum Heist: A Technical Analysis of the March 2025 Security Incident

1. Executive Summary:
   On February 21, 2025, the cryptocurrency exchange Bybit experienced a significant security breach resulting in the theft of approximately $1.5 billion in Ethereum tokens, marking the largest cryptocurrency heist in history.1 The attack has been attributed to the Lazarus Group, also known as TraderTraitor, a notorious North Korean hacking collective.1 The attackers exploited vulnerabilities within Safe{Wallet}, a third-party multisignature platform utilized by Bybit for securing its digital assets.1 The methods employed involved a sophisticated blend of social engineering tactics targeting a Safe{Wallet} developer and the injection of malicious JavaScript code to manipulate transaction interfaces.1 Following the successful theft, the perpetrators initiated a rapid and complex money laundering operation, primarily utilizing decentralized exchanges (DEXs) and cross-chain bridges to obscure the flow of funds.1
   The unprecedented scale of this cryptocurrency theft, coupled with the swift and sophisticated laundering process, underscores the growing capabilities of state-sponsored cybercriminal groups like the Lazarus Group. Their proficiency in identifying and exploiting security weaknesses, combined with their advanced money laundering techniques, poses a significant and evolving threat to the cryptocurrency ecosystem. The ability to move such a substantial amount of funds so quickly through illicit channels highlights the urgent need for enhanced security protocols and international cooperation within the digital asset space.
2. Introduction:
   Bybit has established itself as a prominent player in the global cryptocurrency exchange market, recognized as one of the largest platforms by trading volume.1 The cryptocurrency ecosystem, while offering innovative financial solutions, faces increasing threats from sophisticated cyberattacks, particularly targeting exchanges that manage substantial volumes of digital assets.1 This report delves into the specifics of the unprecedented Ethereum theft from Bybit in March 2025, an incident that stands as the largest cryptocurrency heist recorded to date.1
3. Incident Timeline:
   The security incident targeting Bybit's Ethereum reserves unfolded over several weeks, commencing with the initial compromise of a critical third-party vendor.
   - **February 4, 2025:** The earliest stage of the attack involved the likely social engineering of a Safe{Wallet} developer. This individual's macOS workstation was compromised, potentially through a malicious Docker project that the developer unwittingly downloaded and executed, believing it to be legitimate

software.[2] Analysis indicated that this Docker project, bearing names like "MC-Based-Stock-Invest-Simulator-main" or similar, initiated network traffic towards suspicious domains, such as getstockprice[.]com.[7] This initial compromise likely resulted in the installation of a remote access trojan (RAT) on the developer's system.[55]

- **February 5-17, 2025:** Following the initial compromise, the attackers leveraged stolen AWS session tokens from the infected developer's machine to gain unauthorized access to Safe{Wallet}'s Amazon Web Services (AWS) account.[2] The attackers then operated within this environment for approximately two weeks, engaging in reconnaissance activities to understand the system's architecture and identify potential vulnerabilities, while also meticulously planning their subsequent actions.[2] During this period, there was a recorded failed attempt by the attackers to register an additional Multi-Factor Authentication (MFA) device to the compromised developer account.[2] The attackers' activity within the AWS environment was reportedly traced to ExpressVPN IP addresses, utilizing a user-agent string indicative of a Kali Linux distribution, a common operating system for security professionals and threat actors alike.[7]
- **February 17, 2025:** The attackers proceeded to inject malicious JavaScript code into the source code of Safe{Wallet}'s web interface. This code was hosted on an AWS Simple Storage Service (S3) bucket, specifically targeting the app.safe[.]global domain.[2]
- **February 19, 2025:** Further modifications were made to the malicious JavaScript resources residing on the AWS S3 bucket.[7]
- **February 21, 2025 (around 12:30 PM UTC):** On the day of the heist, Bybit initiated what appeared to be a routine transfer of Ethereum from its cold wallet to a hot wallet using the compromised Safe{Wallet} interface.[1]
- **February 21, 2025 (14:13:35 UTC):** The malicious JavaScript code, which had been lying dormant, activated during this transaction. It manipulated the smart contract logic in real-time, deceiving the Bybit employees who were approving the transfer.[7]
- **February 21, 2025 (shortly after 14:13:35 UTC):** As a result of the manipulated transaction, over 400,000 ETH, along with other tokens including stETH, mETH, and cmETH, with a total value of approximately $1.5 billion, were illicitly transferred to attacker-controlled addresses.[1]
- **February 21, 2025 (14:15 UTC):** A mere two minutes after the malicious transaction was executed, the malicious JavaScript code was removed from Safe{Wallet}'s web interface. This action was likely undertaken by the attackers in an attempt to conceal their intrusion and hinder subsequent

forensic analysis.[7]

- **February 22, 2025:** The day following the attack, Bybit's CEO, Ben Zhou, publicly confirmed the security breach. In a move to encourage the recovery of the stolen assets, he also announced the launch of a bounty program, offering a significant reward for any information or assistance leading to the retrieval of the misappropriated funds.[5]
- **February 26, 2025:** Following initial investigations by Bybit and blockchain analytics firms, the Federal Bureau of Investigation (FBI) officially attributed the massive cryptocurrency theft to the Lazarus Group, a state-sponsored hacking organization with ties to North Korea. The FBI referred to this specific malicious cyber activity as "TraderTraitor".[1]
- **March 7, 2025:** Approximately two weeks after the incident, Safe{Wallet} released a preliminary report detailing the findings of their internal investigation. The report confirmed that a developer's machine had been compromised, allowing the attackers to manipulate the user interface and execute the fraudulent transaction. Safe{Wallet} also disclosed that they had engaged Google Cloud's Mandiant for further forensic analysis.[21]

4. Attack Vector Analysis:
   The attack on Bybit's Ethereum reserves was a multifaceted operation that leveraged vulnerabilities across several layers of the targeted infrastructure.
   - **Initial Compromise of Safe{Wallet} Infrastructure (Social Engineering):** The initial breach into the Safe{Wallet} ecosystem is strongly believed to have been facilitated through social engineering tactics directed at a Safe{Wallet} developer. This likely involved the developer being tricked into downloading and executing a seemingly harmless, yet malicious, Docker project.[2] These projects, often disguised as legitimate stock investment simulators or similar tools, contained malicious software.[55] Once executed, these projects established network connections to suspicious domains, such as getstockprice[.]com, and likely installed a remote access trojan (RAT) on the developer's workstation.[7]
   - **Unauthorized Access to AWS Environment:** With the developer's machine compromised, the attackers were able to steal active AWS session tokens, granting them unauthorized access to Safe{Wallet}'s AWS infrastructure.[2] This access, reportedly originating from ExpressVPN IP addresses and using a Kali Linux user-agent string, persisted for approximately two weeks prior to the actual theft.[7] During this period, the attackers attempted to further secure their access by registering an additional MFA device but were unsuccessful.[2]
   - **Malicious JavaScript Injection and Manipulation of Transaction Interface:** Leveraging their access to Safe{Wallet}'s AWS environment, the

attackers injected malicious JavaScript code into the web interface code hosted on an S3 bucket.[2] This code was specifically crafted to target Bybit's cold wallet transactions, particularly the routine transfers from the cold wallet to the hot wallet.[2] The injected JavaScript manipulated the transaction interface presented to the Bybit employees, displaying the correct destination address and amount for a legitimate transfer while simultaneously altering the underlying smart contract logic to redirect the funds to wallets controlled by the attackers.[1] Crucially, the malicious JavaScript was designed to revert the displayed transaction data to the original intended details immediately after the signers had approved the tampered transaction, further masking the attack.[30]

- **Exploitation of Smart Contract Functionality (Delegatecall):** The core of the on-chain exploit involved the misuse of the delegatecall function within the Gnosis Safe smart contract, which underpins Safe{Wallet}.[7] This function allows a smart contract to execute code from another contract while maintaining the storage context of the calling contract. The attackers crafted a transaction that, when approved by the Bybit signers, invoked the delegatecall function on Bybit's cold wallet proxy contract.[7] The target of this delegatecall was a pre-deployed malicious smart contract controlled by the attackers.[7] The code within this malicious contract was designed to modify the storage slot 0 of Bybit's cold wallet proxy contract, which holds the address of the implementation contract (referred to as masterCopy).[7] By overwriting this pointer with the address of their own malicious contract, the attackers effectively gained complete control over Bybit's cold wallet, enabling them to execute arbitrary functions, including those for sweeping ETH and ERC-20 tokens.[7]

5. Technical Details of the Exploit:
   The exploit involved a carefully orchestrated sequence of off-chain and on-chain manipulations.
   - **Analysis of the Malicious JavaScript Code:** The injected JavaScript code was designed with specific functionalities to facilitate the attack. Firstly, it verified if the user initiating the transaction was one of Bybit's authorized signers.[30] If the user was not authorized, the application would function normally. Upon identifying an authorized signer preparing a transaction, the script would create a backup of the original transaction data that was intended for signing.[30] Subsequently, it would replace this original data with a modified operation. This modification involved changing the to field to the attacker's designated contract address (0x96221423681A6d52E184D440a8eFCEbB105C7242), altering the data field

to a specific function call (0xa9059cbb000000000000000000000000bdd077f651ebe7f7b3ce16fe5f2b025be2969516000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000), setting the operation parameter to 1 (indicating a delegatecall), the value to 0, and the safeTxGas to 45746.[30] The tampered transaction data was then presented to the signer for approval through their wallet. Critically, after the signer had approved the malicious transaction within their wallet, the JavaScript script would revert the transaction object back to the *original* transaction data. However, it retained the signature that had been obtained for the tampered transaction. This tampered signature, now associated with the original (but off-chain altered) transaction details, was then shared with the remaining signers.[30] The malicious code also incorporated an activation condition that ensured its execution only when the transaction originated from Bybit's specific cold wallet contract address.[7] Additionally, the transaction validation function within the JavaScript was tampered with to bypass security checks on the transaction and its digital signatures.[7]

- **Smart Contract Interaction and the Delegatecall Mechanism:** Bybit's cold wallet operated as a proxy contract, meaning it delegated all function calls to an implementation contract. In this case, the proxy contract at address 0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4 was configured to delegate calls to the Gnosis Safe masterCopy contract located at 0x34CfAC646f301356fAa8B21e94227e3583Fe3F5F.[30] The attacker, prior to the heist, had deployed a seemingly simple smart contract at address 0x96221423681A6d52E184D440a8eFCEbB105C7242.[30] This attacker contract contained a function with the same signature as an ERC-20 transfer(address, uint256) function. However, instead of performing a token transfer, this function was designed to modify the value stored in storage slot 0 of the contract's storage to the address provided in the _to parameter. The malicious transaction that initiated the exploit called the execTransaction function of the Gnosis Safe masterCopy contract. This call included tampered parameters: the to field was set to the attacker's contract address, the data field contained the encoded call to the transfer function within the attacker's contract, the operation parameter was set to 1 (delegatecall), and the safeTxGas was set to 45746.[30] The sequence of events on the blockchain was as follows: First, the Bybit cold wallet (the proxy contract) delegated the execution of the call to the Gnosis Safe (the masterCopy contract). The Gnosis Safe contract then verified that the provided signatures were valid for the given parameters. Due to the operation parameter being set to 1, the

Gnosis Safe contract then delegated the execution of the data specified in the data parameter to the contract address provided in the to field, which was the attacker's contract. The decoded data instructed the attacker's contract to call its transfer function with the _to parameter set to 0xbDd077f651EBe7f7b3cE16fe5F2b025BE2969516 and the _value set to 0. Because of the delegatecall, the attacker's contract executed within the storage context of the Bybit cold wallet (the proxy contract). The transfer function in the attacker's contract then modified storage slot 0 of the Bybit cold wallet, which contained the address of the masterCopy, to the attacker's chosen address: 0xbDd077f651EBe7f7b3cE16fe5F2b025BE2969516. Once this transaction was confirmed on the blockchain, the implementation pointer of the Bybit cold wallet proxy contract was under the control of the attackers. This allowed them to execute arbitrary code and subsequently steal all the funds held within the contract.

- **Use of Specific Technical Names, Packages, and Frameworks:** The attack leveraged a combination of prominent technologies within the cryptocurrency and software development landscape. **Safe{Wallet}**, formerly known as Gnosis Safe, served as the multisignature wallet platform employed by Bybit for securing its digital assets.[1] The infrastructure of Safe{Wallet}, including the storage of its web interface code, was hosted on **AWS (Amazon Web Services)**.[2] The user interface itself was developed using **JavaScript**, which was the programming language targeted for malicious code injection.[1] The smart contracts involved, including Bybit's cold wallet, the Gnosis Safe contract, and the attacker's malicious contract, were written in **Solidity** (implicitly). The compromised developer's environment utilized **Docker**, a containerization platform, which was likely the vector for the initial malware deployment.[2] Furthermore, the initial intrusion likely involved the exploitation of **pyyaml**, a Python library, for achieving remote code execution.[55] Finally, the attackers reportedly deployed **MythicAgents**, an open-source offensive framework, during their operation.[7]

6. Common Vulnerabilities and Exposures (CVE) Record Investigation:
   An investigation into publicly available vulnerability databases did not reveal a specific Common Vulnerabilities and Exposures (CVE) record directly associated with the Bybit hack or the compromise of Safe{Wallet} at the time of the incident. However, reports indicate that the initial access to the Safe{Wallet} developer's machine likely involved the exploitation of known vulnerabilities within the pyyaml library. Specifically, CVE-2020-1747 and CVE-2020-14343, both critical vulnerabilities allowing for arbitrary code execution when processing untrusted YAML files, are relevant in this context.55 These vulnerabilities could have been

leveraged through the malicious Docker project to execute code on the developer's machine, leading to the subsequent compromise. It is important to note that while these CVEs relate to the initial intrusion vector, no specific CVE was identified in the provided research material for the subsequent compromise of Safe{Wallet}'s AWS infrastructure or the manipulation of the smart contract logic that directly resulted in the theft of Ethereum. This absence could potentially be attributed to the ongoing nature of the investigation at the time the research material was published, or possibly due to a backlog in the assignment and processing of CVE records, as suggested by reports of delays within the National Vulnerability Database (NVD) during March 2025.128

7. Laundering of Stolen Ethereum:
   Following the successful theft of Ethereum and other tokens, the attackers initiated a rapid and multifaceted money laundering process to obscure the origin and flow of the ill-gotten gains. A primary step in this process involved the swift exchange of the stolen ETH for Bitcoin and other virtual assets.2 The stolen funds were then dispersed across a vast network of thousands of cryptocurrency addresses, spanning multiple blockchain platforms.3 The laundering process heavily relied on decentralized exchanges (DEXs), such as THORChain, which facilitated direct asset swaps without the need for intermediaries.1 Additionally, cross-chain bridges were utilized to move assets between different blockchain networks, further complicating the tracing of funds. Cryptocurrency mixers, including services like Wasabi and CryptoMixer, were also employed to obscure the transaction trail by pooling and redistributing crypto assets, making it difficult to link the origin and destination of the stolen funds.1 Initially, some of the stolen Ethereum was routed through networks such as Binance Smart Chain and Solana 5, but the majority was ultimately converted directly into Bitcoin.2 The attackers also employed a "flood the zone" technique, characterized by rapid and high-frequency transactions across numerous platforms, likely to overwhelm compliance teams and blockchain analysts.2 Reports even suggest the potential involvement of money laundering-as-a-service providers, indicating a sophisticated and organized approach to handling the stolen funds.2
8. Incident Response and Security Enhancements:
   Following the detection of the security breach, both Bybit and Safe{Wallet} initiated incident response protocols and began implementing measures to address the situation and prevent future occurrences.
   - **Bybit's Public Statements and Actions Taken:** Bybit's CEO, Ben Zhou, promptly addressed the incident, assuring the exchange's users that Bybit remained financially solvent and that all withdrawals were functioning normally.[1] To facilitate the recovery of the stolen assets, Bybit launched a

bounty program, offering a 10% reward for any successful leads or assistance in retrieving the funds.[5] Bybit actively collaborated with numerous blockchain analytics firms, including TRM Labs, Chainalysis, Elliptic, Crystal Intelligence, and Arkham Intelligence, as well as law enforcement agencies like the FBI, to track the movement of the stolen funds and aid in their potential recovery.[1] These efforts led to the reported freezing of a portion of the stolen funds.[5] To ensure the continued availability of user funds despite the significant loss, Bybit secured bridge loans from various partners [14] and successfully replenished its ETH reserves.[6] Furthermore, Bybit developed a new API system designed to track and detect blacklisted wallets in real-time, enhancing their ability to monitor and potentially recover funds.[100]

- **Security Measures Implemented by Bybit Following the Incident:** In response to the attack, Bybit announced and implemented several enhanced security measures aimed at fortifying its platform against future threats. These measures included the reinforcement of two-factor authentication (2FA) across all user accounts [88], the enhancement of data encryption protocols [88], and a strategic shift to storing a greater percentage of user funds in cold wallets, which are offline and less accessible to cyber threats.[88] Bybit also implemented advanced real-time monitoring systems to improve the detection of suspicious activities on the platform [88] and initiated an evaluation of alternative wallet solutions to ensure the highest standards of security for user assets.[95] Additionally, stricter API security protocols were put in place to protect against unauthorized access and manipulation.[97]
- **Security Updates and Recommendations from Safe{Wallet}:** Safe{Wallet} responded to the incident by engaging Mandiant, a leading cybersecurity firm, to conduct a comprehensive forensic investigation into the attack.[35] Following the initial findings, Safe{Wallet} undertook a complete rebuilding and reconfiguration of its infrastructure, including the rotation of all access credentials, to eliminate the identified attack vector.[91] To enhance transaction security, stricter checks were implemented for transaction hashes, data, and digital signatures to ensure their authenticity and integrity.[102] As the compromised signing method in the Bybit attack involved a Ledger device, Safe{Wallet} temporarily removed native Ledger integration as a precautionary measure.[102] The platform now supports customizable multisignature thresholds, allowing users to require multiple approvals for transactions, a feature particularly beneficial for institutional clients and decentralized autonomous organizations (DAOs).[102] Safe{Wallet} is also in the process of integrating an AI-driven monitoring system to scan for and alert users about suspicious activities in real-time.[102] Furthermore, Safe{Wallet}

reiterated the critical importance of users carefully verifying all transaction data before signing and committed to leading an industry-wide initiative aimed at increasing the overall verifiability of cryptocurrency transactions, recognizing this as a significant challenge across the entire ecosystem.[35]

9. Attribution to North Korean Hackers (Lazarus Group/TraderTraitor):
   The Federal Bureau of Investigation (FBI), along with numerous prominent blockchain analytics firms such as TRM Labs, Elliptic, Chainalysis, and Arkham Intelligence, have attributed the sophisticated cyberattack on Bybit to the Lazarus Group, a notorious state-sponsored hacking organization with strong ties to North Korea.1 This attribution is supported by several key pieces of evidence, including significant overlaps in the cryptocurrency wallet addresses used in the Bybit attack with those previously linked to other cyber heists orchestrated by North Korean actors.5 Furthermore, the tactics, techniques, and procedures (TTPs) observed in the Bybit attack bear a striking resemblance to those historically employed by the Lazarus Group in their previous operations. These include the use of social engineering to gain initial access, the deployment of sophisticated phishing campaigns and malware, and the execution of rapid and intricate money laundering schemes to obfuscate the stolen funds.1 The Lazarus Group has a well-established history of engaging in state-sponsored cyber activities, primarily aimed at generating revenue to fund North Korea's nuclear and ballistic missile programs, making cryptocurrency exchanges a frequent target due to the substantial financial gains achievable.1 The sheer magnitude of the Bybit heist aligns with the Lazarus Group's known preference for high-impact operations, often targeting large cryptocurrency platforms to maximize their illicit profits.5 Further corroborating the Lazarus Group's involvement, researchers discovered that a domain named "bybit-assessment[.]com" was registered mere hours before the Bybit hack. This domain was found to be linked to an email address previously associated with Lazarus Group activities, and logs from the attackers' infrastructure even contained a test entry using a name closely resembling "Lazarus".15
10. Conclusion:
    The security incident that resulted in the theft of approximately $1.5 billion in Ethereum from Bybit in February 2025 represents a watershed moment in the history of cryptocurrency heists. The sheer scale of the attack, the largest of its kind to date, underscores the persistent and evolving threats facing the digital asset ecosystem. The attack vector, which involved a sophisticated supply chain compromise targeting a third-party vendor, Safe{Wallet}, highlights the interconnectedness of the cryptocurrency infrastructure and the potential vulnerabilities that can arise from reliance on external service providers. The

technical execution of the exploit demonstrated a high level of skill, combining social engineering, malicious JavaScript injection to manipulate the user interface, and a clever exploitation of the delegatecall functionality within the Gnosis Safe smart contract. The attackers' ability to deceive Bybit employees into approving a fraudulent transaction, despite the presence of multisignature security measures, underscores the critical importance of robust transaction verification processes that extend beyond the visual representation provided by user interfaces. The rapid and complex money laundering operation that followed the theft further illustrates the challenges faced by law enforcement and blockchain analytics firms in tracking and recovering stolen cryptocurrency. The strong attribution of this attack to the North Korean Lazarus Group, based on compelling evidence such as overlapping wallet addresses, similar TTPs, and the geopolitical context of North Korea's cybercriminal activities, underscores the state-sponsored nature of this threat and the significant resources and expertise behind such operations. This incident carries profound implications for the security of cryptocurrency exchanges and the broader digital asset ecosystem. It emphasizes the imperative for enhanced security measures across the industry, including more rigorous oversight of third-party vendors, the implementation of multi-layered transaction verification protocols, and the proactive sharing of threat intelligence to better anticipate and mitigate sophisticated attacks. As state-sponsored cybercriminals continue to refine their tactics and target high-value cryptocurrency holdings, a paradigm shift in security practices is essential to build a more resilient and trustworthy digital asset ecosystem.

11. **References:**

    - https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation
    - https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now
    - https://www.ic3.gov/psa/2025/psa250226
    - https://www.trmlabs.com/resources/blog/bybit-hack-update-north-korea-moves-to-next-stage-of-laundering
    - https://www.picussecurity.com/resource/blog/fbi-north-korean-lazarus-group-bybit-crypto-heist
    - https://www.trmlabs.com/resources/blog/the-bybit-hack-following-north-koreas-largest-exploit
    - https://areteir.com/article/bybit-ethereum-theft-2025-crypto-heist/
    - https://www.nknews.org/pro/tools-of-the-trade-how-north-korea-launders-billions-in-stolen-cryptocurrency/
    - https://www.blockscholes.com/research/bybit-incident-postmortem-how-bybit-rose-from-the-hack-and-protects-its-rpi-retail-users
    - https://www.fintechweekly.com/magazine/articles/bybit-ceo-ben-zhou-says-

most-funds-are-still-traceable
- https://www.oligo.security/blog/bybit-1-5b-crypto-heist-adr-best-practices-and-lessons-learned
- https://www.paulhastings.com/insights/crypto-policy-tracker/the-bybit-hack-of-2025-potential-implications
- https://www.ledgerinsights.com/bybit-crypto-hack-safe-wallet-reveals/
- https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/
- https://www.voanews.com/a/north-korea-behind-1-5-billion-crypto-theft-fbi-says/7989814.html
- https://cyberscoop.com/bybit-lazarus-group-north-korea-ethereum/
- https://www.nccgroup.com/us/research-blog/in-depth-technical-analysis-of-the-bybit-hack/
- https://www.elliptic.co/blog/bybit-hack-largest-in-history
- https://crystalintelligence.com/investigations/breaking-down-the-bybit-exchange-hack/
- https://www.brigantia.com/resources/march-2025-cybersecurity-round-up
- https://thehackernews.com/2025/02/bybit-confirms-record-breaking-146.html?m=0
- https://nvd.nist.gov/vuln/detail/CVE-2025-32013
- https://www.cisa.gov/news-events/bulletins/sb25-041
- https://www.cm-alliance.com/cybersecurity-blog/february-2025-major-cyber-attacks-ransomware-attacks-data-breaches
- https://www.cisa.gov/news-events/bulletins/sb25-049
- https://protosnetworks.com/cyber-news-february-2025/
- https://strobes.co/blog/top-cves-vulnerabilities-february-2025/
- https://socradar.io/major-cyber-attacks-in-review-february-2025/
- https://ctichef.com/cybersec-feeds/20250223/?utm_source=feedly
- https://avoidthehack.com/privacy-week7-2025
- https://telefonicatech.com/en/blog/cyber-security-briefing-22-28-february-2025
- https://visionspace.com/remote-code-execution-via-man-in-the-middle-and-more-in-nasas-ait-core-v2-5-2/
- https://www.ibm.com/support/pages/security-bulletin-vulnerability-pyyaml-affects-ibm-spectrum-protect-plus-container-and-microsoft-file-systems-agents-cve-2020-1747
- https://www.cve.org/CVERecord?id=CVE-2020-1747
- https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=PyYAML
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1747
- https://nvd.nist.gov/vuln/detail/cve-2020-14343

- https://www.cvedetails.com/cve/CVE-2020-14343/
- https://semgrep.dev/blog/2022/testing-vulnerable-pyyaml-versions/
- https://github.com/advisories/GHSA-8q59-q68h-6hv4
- https://nvd.nist.gov/vuln/detail/cve-2020-1747
- https://www.kaspersky.com/blog/bybit-hack-lessons-how-to-do-self-custody-properly/53155/
- https://www.halborn.com/blog/post/what-the-bybit-hack-reveals-about-blockchain-aml-weaknesses
- https://blog.checkpoint.com/security/what-the-bybit-hack-means-for-crypto-security-and-the-future-of-multisig-protection/
- https://quant.network/perspectives/the-need-for-enterprise-security-measures-in-the-wake-of-the-bybit-attack/
- https://www.anchain.ai/blog/bybit
- https://www.dfns.co/article/the-bybit-safe-hack
- https://thehackernews.com/2025/03/safewallet-confirms-north-korean.html
- https://www.bovill-newgate.com/americas/breaking-the-vault-lessons-in-custody-security-from-the-bybit-hack/
- https://www.cyfrin.io/blog/safe-wallet-hack-bybit-exploit
- https://www.ledgerinsights.com/bybit-hack-phishing-involved-plus-how-to-prevent-similar-hacks/
- https://www.indrastra.com/2025/02/bybit-suffers-historic-14-billion-hack.html
- https://www.pymnts.com/cryptocurrency/2025/crypto-theft-sees-303-percent-quarterly-jump-after-record-bybit-hack/
- https://research.kaiko.com/insights/bybit-hack-by-the-numbers
- https://www.gemini.com/blog/bybit-hack-shakes-crypto-market-ethereum-prepares-for-pectra-update-and-sec
- https://www.fintechweekly.com/magazine/articles/bybit-hack
- https://insights.glassnode.com/the-week-onchain-week-08-2025/
- https://research.checkpoint.com/2025/the-bybit-incident-when-research-meets-reality/
- https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now
- https://www.cobo.com/post/the-bybit-breach-why-multi-sig-alone-isn-t-enough
- https://thehackernews.com/2025/04/lazarus-group-targets-job-seekers-with.html
- https://www.rfa.org/english/korea/2025/02/27/north-korea-lazarus-bybit-cryptocurrency-theft/
- https://www.radware.com/cyberpedia/ddos-attacks/the-lazarus-group-apt38-north-korean-threat-actor/

- https://www.grip.globalrelay.com/lessons-learned-from-the-bybit-hack-a-forensic-accountants-perspective/
- https://cointelegraph.com/learn/articles/lessons-from-bybit-hack-how-to-stay-safe
- https://www.quillaudits.com/blog/web3-security/bybit-hack-security-lesson
- https://www.onesafe.io/blog/bybit-hack-lessons-cryptocurrency-security-dea6b
- https://reinasia.com/the-bybit-hack-a-digital-asset-insurance-perspective-and-lessons-learned/
- https://www.scworld.com/perspective/the-bybit-hack-a-crypto-heist-with-cloud-security-lessons
- https://blog.trailofbits.com/2025/02/21/the-1.5b-bybit-hack-the-era-of-operational-security-failures-has-arrived/
- https://coinmarketcap.com/academy/article/0679167d-8558-441b-96e8-8345794eff9e
- https://coinbureau.com/analysis/is-kraken-safe/
- https://www.security.org/digital-security/crypto/
- https://www.getfocal.ai/blog/cryptocurrency-transaction-monitoring
- https://www.efani.com/blog/crypto-security
- https://www.bitcoin.com/decentralized-exchanges/best-practices/
- https://www.grantthornton.com/insights/articles/advisory/2025/crypto-policy-outlook
- https://blog.trailofbits.com/2025/02/05/preventing-account-takeover-on-centralized-cryptocurrency-exchanges-in-2025/
- https://www.chainalysis.com/blog/preventing-crypto-hacks-best-practices-for-exchanges-hexagate/
- https://www.moneylaunderingnews.com/2025/03/recent-developments-raise-significant-questions-about-the-future-of-regulation-and-enforcement-of-cryptocurrency/
- https://www.silentpush.com/blog/lazarus-bybit/
- https://thehackernews.com/2025/03/safewallet-confirms-north-korean.html
- https://www.halborn.com/blog/post/explained-the-bybit-hack-revisited
- https://news.risky.biz/risky-bulletin-north-korean-hackers-steal-1-5-billion-from-bybit/
- https://www.reflectiz.com/blog/bybit-crypto-hack/
- https://kaironlabs.com/blog/the-bybit-usd1-5b-hack-a-masterclass-in-crisis-management
- https://crystalintelligence.com/investigations/the-bybit-heist-how-the-hackers-took-control/

- https://blockchaintechnology-news.com/news/how-lazarus-group-became-a-global-cybercrime-threat-from-sony-to-bybit/
- https://research.checkpoint.com/2025/the-bybit-incident-when-research-meets-reality/
- https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now
- https://www.cobo.com/post/cobo-at-cyberport-2025-dissecting-the-bybit-breach-and-the-future-of-wallet-security
- https://blogs.usfcr.com/bybit-hack-cybersecurity-response
- https://announcements.bybit.com/article/bybit-s-security-update-asset-recovery-and-enhanced-security-measure-blt47be62971e11fb74/
- https://announcements.bybit.com/article/incident-update---eth-cold-wallet-incident-blt292c0454d26e9140/
- https://www.bleepingcomputer.com/news/security/lazarus-hacked-bybit-via-breached-safe-wallet-developer-machine/
- https://news.risky.biz/risky-bulletin-north-korean-hackers-steal-1-5-billion-from-bybit/
- https://www.binance.com/en/square/post/03-06-2025-bybit-hack-safewallet-report-reveals-details-of-1-4-billion-cybersecurity-breach-21195682977506
- https://www.tradingview.com/news/cointelegraph:108027933094b:0-safewallet-releases-bybit-hack-post-mortem-report/
- https://safe.global/blog/safe-ecosystem-foundation-statement
- https://ackee.xyz/blog/a-safe-native-solution-to-the-bybit-hack/
- https://ecos.am/en/blog/best-crypto-wallets-for-2025-security-features-and-expert-recommendations/
- https://safe.global/wallet
- https://safe.global/blog/best-cold-storage-wallets
- https://crypto.news/safe-wallet-security-features-bybit-hack-2025/
- https://patrickalphac.medium.com/top-9-cryptocurrency-hardware-wallets-for-2025-security-researcher-review-9fcb16d771e0
- https://hackread.com/crypto-wallets-2025-balancing-security-convenience/
- https://milkroad.com/reviews/safe-wallet/
- https://www.morningstar.com/news/pr-newswire/20250226cn28105/bybit-confirms-security-integrity-amid-safe-wallet-incident-no-compromise-in-infrastructure
- https://www.financemagnates.com/cryptocurrency/bybit-14-billion-breach-linked-to-safe-wallet-vulnerability-investigation-finds/
- https://techpoint.africa/guide/bybit-hack-2025/
- https://www.reddit.com/r/ethereum/comments/1iw6jbn/explain_me_bybit_hack_like_i_am_6_years_old/

- https://www.youtube.com/watch?v=jq9y9KmSlr0
- https://www.youtube.com/watch?v=QdXCYmN7nDg
- https://www.elliptic.co/blog/a-race-against-time-how-elliptics-real-time-intelligence-is-recovering-funds-from-historys-largest-crypto-hack
- https://www.elliptic.co/bybit-exploit-blocklist
- https://therecord.media/north-koreans-initial-laundering-bybit-hack
- https://www.nbcconnecticut.com/news/business/money-report/hackers-steal-1-5-billion-from-exchange-bybit-in-biggest-ever-crypto-heist/3505003/
- https://www.elliptic.co/media-center/elliptic-data-used-by-us-secret-service-in-investigation-into-60-billion-russian-crypto-exchange-garantex
- https://www.analyse.asia/the-lazarus-group-the-bybit-hack-and-sanctions-the-new-battleground-chainalysis-andrew-fierman/
- https://www.anchain.ai/investigations
- https://www.anchain.ai/security
- https://www.anchain.ai/
- https://www.anchain.ai/training
- https://news.risky.biz/risky-bulletin-north-korean-hackers-steal-1-5-billion-from-bybit/
- https://therecord.media/north-koreans-initial-laundering-bybit-hack
- https://www.sygnia.co/blog/

Date	Event	Snippet IDs
February 4, 2025	Compromise of a Safe{Wallet} developer's macOS workstation	2
February 5-17, 2025	Attackers access Safe{Wallet}'s AWS account, conduct reconnaissance	2
February 17, 2025	Malicious JavaScript injected into Safe{Wallet}'s UI code on AWS S3	2
February 19, 2025	Malicious JavaScript resources modified on AWS S3	7

February 21, 2025 (around 12:30 PM UTC)	Bybit initiates routine ETH transfer using Safe{Wallet}	1
February 21, 2025 (14:13:35 UTC)	Malicious code activates, altering smart contract logic	7
February 21, 2025 (shortly after 14:13:35 UTC)	Over 400,000 ETH and other tokens transferred to attackers	1
February 21, 2025 (14:15 UTC)	Malicious JavaScript code removed from Safe{Wallet}'s web interface	7
February 22, 2025	Bybit CEO confirms hack and announces bounty program	5
February 26, 2025	FBI attributes attack to North Korea's Lazarus Group (TraderTraitor)	1
March 7, 2025	Safe{Wallet} releases preliminary investigation report	21

Works cited

1. The ByBit Heist and the Future of U.S. Crypto Regulation - CSIS, accessed on April 11, 2025, https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation
2. The Bybit Heist: What Happened & What Now? | Wilson Center, accessed on April 11, 2025, https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now
3. North Korea Responsible for $1.5 Billion Bybit Hack - Internet Crime Complaint Center, accessed on April 11, 2025, https://www.ic3.gov/psa/2025/psa250226
4. FBI Confirms North Korean Lazarus Group Behind $1.5 Billion Bybit Crypto Heist, accessed on April 11, 2025, https://www.picussecurity.com/resource/blog/fbi-north-korean-lazarus-group-bybit-crypto-heist
5. The Bybit Hack: Following North Korea's Largest Exploit | TRM Blog, accessed on April 11, 2025, https://www.trmlabs.com/resources/blog/the-bybit-hack-following-north-koreas-largest-exploit
6. Bybit Ethereum Theft 2025: $1.4B Stolen in Crypto Heist - Arete, accessed on April

11, 2025, https://areteir.com/article/bybit-ethereum-theft-2025-crypto-heist/
7. Sygnia's Investigation into the Bybit Hack: What We Know So Far, accessed on April 11, 2025, https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/
8. Lazarus Group Steals $1.5 Billion – Cyber, accessed on April 11, 2025, https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/lazarus-group-steals-1-5-billion/
9. North Korea Responsible for $1.5 Billion Bybit Hack - Internet Crime Complaint Center, accessed on April 11, 2025, https://www.ic3.gov/PSA/2025/PSA250226?ref=infophreak.com
10. North Korea behind $1.5 billion crypto theft, FBI says - VOA, accessed on April 11, 2025, https://www.voanews.com/a/north-korea-behind-1-5-billion-crypto-theft-fbi-says/7989814.html
11. Crypto analysts stunned by Lazarus Group's capabilities in $1.46B Bybit theft | CyberScoop, accessed on April 11, 2025, https://cyberscoop.com/bybit-lazarus-group-north-korea-ethereum/
12. Cyber News February 2025 - Protos Networks, accessed on April 11, 2025, https://protosnetworks.com/cyber-news-february-2025/
13. Major Cyber Attacks in Review: February 2025 - SOCRadar® Cyber Intelligence Inc., accessed on April 11, 2025, https://socradar.io/major-cyber-attacks-in-review-february-2025/
14. Bybit Hack Shakes Crypto Market, Ethereum Prepares for Pectra Update, and SEC Eases Up On Crypto | Gemini, accessed on April 11, 2025, https://www.gemini.com/blog/bybit-hack-shakes-crypto-market-ethereum-prepares-for-pectra-update-and-sec
15. Silent Push Pivots into New Lazarus Group Infrastructure, Acquires Sensitive Intel Related to $1.4B ByBit Hack and Past Attacks, accessed on April 11, 2025, https://www.silentpush.com/blog/lazarus-bybit/
16. Lazarus Group Targets Job Seekers With ClickFix Tactic to Deploy GolangGhost Malware, accessed on April 11, 2025, https://thehackernews.com/2025/04/lazarus-group-targets-job-seekers-with.html
17. North Korean hackers behind largest ever financial theft - Radio Free Asia, accessed on April 11, 2025, https://www.rfa.org/english/korea/2025/02/27/north-korea-lazarus-bybit-cryptocurrency-theft/
18. The Lazarus Group (APT38): North Korean Threat Actor - Radware, accessed on April 11, 2025, https://www.radware.com/cyberpedia/ddos-attacks/the-lazarus-group-apt38-north-korean-threat-actor/
19. The Bybit Hack of 2025 — Potential Implications | Paul Hastings LLP, accessed on April 11, 2025, https://www.paulhastings.com/insights/crypto-policy-tracker/the-bybit-hack-of-2025-potential-implications
20. How Lazarus Group became a global cybercrime threat from Sony to Bybit -

Blockchain News, accessed on April 11, 2025, https://blockchaintechnology-news.com/news/how-lazarus-group-became-a-global-cybercrime-threat-from-sony-to-bybit/
21. Explained: The Bybit Hack Revisited - Halborn, accessed on April 11, 2025, https://www.halborn.com/blog/post/explained-the-bybit-hack-revisited
22. North Korean hackers steal $1.5 billion from Bybit - Risky Biz News, accessed on April 11, 2025, https://news.risky.biz/risky-bulletin-north-korean-hackers-steal-1-5-billion-from-bybit/
23. The $1.5 Billion Bybit Hack: Lessons from History's Largest Crypto Heist - Reflectiz, accessed on April 11, 2025, https://www.reflectiz.com/blog/bybit-crypto-hack/
24. Collaboration in the Wake of Record-Breaking Bybit Theft - Chainalysis, accessed on April 11, 2025, https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/
25. FBI accuses North Korea in $1.5B Bybit crypto theft | AP News, accessed on April 11, 2025, https://apnews.com/article/bybit-exchange-crypto-hack-north-korea-7c8335c1397261554138090c2c38f457
26. FBI Confirms North Korea's Lazarus Group as Bybyit Hackers - Infosecurity Magazine, accessed on April 11, 2025, https://www.infosecurity-magazine.com/news/fbi-confirms-north-koreas-lazarus/
27. FBI officially fingers North Korea for $1.5B Bybit crypto-burglary - The Register, accessed on April 11, 2025, https://www.theregister.com/2025/02/27/fbi_bybit_korea/
28. North Korea aims 'TraderTraitor' malware at cryptocurrency workers - CyberScoop, accessed on April 11, 2025, https://cyberscoop.com/tradertraitor-malware-warning-cisa-lazarus-group-north-korea/
29. Behind the Bybit Crypto Theft - Communications of the ACM, accessed on April 11, 2025, https://cacm.acm.org/news/behind-the-bybit-crypto-theft/
30. In-Depth Technical Analysis of the Bybit Hack - NCC Group, accessed on April 11, 2025, https://www.nccgroup.com/us/research-blog/in-depth-technical-analysis-of-the-bybit-hack/
31. The largest theft in history - following the money trail from the Bybit Hack - Elliptic, accessed on April 11, 2025, https://www.elliptic.co/blog/bybit-hack-largest-in-history
32. The Bybit Hack: Following North Korea's Largest Exploit | TRM Insights, accessed on April 11, 2025, https://www.trmlabs.com/post/the-bybit-hack-following-north-koreas-largest-exploit
33. Lazarus hacked Bybit via breached Safe{Wallet} developer machine - Bleeping

Computer, accessed on April 11, 2025, https://www.bleepingcomputer.com/news/security/lazarus-hacked-bybit-via-breached-safe-wallet-developer-machine/
34. Bybit Confirms Record-Breaking $1.5 Billion Crypto Heist in Sophisticated Cold Wallet Attack - The Hacker News, accessed on April 11, 2025, https://thehackernews.com/2025/02/bybit-confirms-record-breaking-146.html
35. Safe{Wallet} Confirms North Korean TraderTraitor Hackers Stole $1.5 Billion in Bybit Heist, accessed on April 11, 2025, https://thehackernews.com/2025/03/safewallet-confirms-north-korean.html
36. Bybit Hack Traced to Safe{Wallet} Supply Chain Attack Exploited by North Korean Hackers, accessed on April 11, 2025, https://thehackernews.com/2025/02/bybit-hack-traced-to-safewallet-supply.html
37. The Lazarus Group, The Bybit Hack and Sanctions: The New Battleground with Andrew Fierman - Analyse Asia, accessed on April 11, 2025, https://www.analyse.asia/the-lazarus-group-the-bybit-hack-and-sanctions-the-new-battleground-chainalysis-andrew-fierman/
38. North Koreans finish initial laundering stage after more than $1 billion stolen from Bybit, accessed on April 11, 2025, https://therecord.media/north-koreans-initial-laundering-bybit-hack
39. Hackers steal $1.5 billion from exchange Bybit in biggest-ever crypto heist - NBC Connecticut, accessed on April 11, 2025, https://www.nbcconnecticut.com/news/business/money-report/hackers-steal-1-5-billion-from-exchange-bybit-in-biggest-ever-crypto-heist/3505003/
40. The Bybit/Safe Hack - Dfns, accessed on April 11, 2025, https://www.dfns.co/article/the-bybit-safe-hack
41. Bybit crypto hack: SAFE Wallet reveals how it happened - Ledger Insights, accessed on April 11, 2025, https://www.ledgerinsights.com/bybit-crypto-hack-safe-wallet-reveals/
42. The Bybit Breach: Why Multi-Sig Alone Isn't Enough and How Cobo Tackles the Challenges, accessed on April 11, 2025, https://www.cobo.com/post/the-bybit-breach-why-multi-sig-alone-isn-t-enough
43. The Safe Wallet Hack That Led to Bybit's $1.4B Heist - Cyfrin, accessed on April 11, 2025, https://www.cyfrin.io/blog/safe-wallet-hack-bybit-exploit
44. How Hackers Stole $1.5 Billion Crypto in an AWS S3 Bucket Exploit - Medium, accessed on April 11, 2025, https://medium.com/@csjcode/how-hackers-stole-1-5-billion-crypto-in-an-aws-s3-bucket-exploit-f0a0ce39ccd0
45. How the Bybit Hack Happened—and How to Prevent the Next One with Seraph - Halborn, accessed on April 11, 2025, https://www.halborn.com/blog/post/how-the-bybit-hack-happened-and-how-to-prevent-the-next-one-with-seraph
46. Bybit hack: phishing involved, plus how to prevent similar hacks (updated) - Ledger Insights, accessed on April 11, 2025, https://www.ledgerinsights.com/bybit-hack-phishing-involved-plus-how-to-prev

ent-similar-hacks/
47. Breaking the vault: Lessons in custody security from the Bybit hack - Bovill Newgate, accessed on April 11, 2025, https://www.bovill-newgate.com/americas/breaking-the-vault-lessons-in-custody-security-from-the-bybit-hack/
48. The Flaw in “Secure” Systems: How Bybit's Attack Exploited Blind Trust - Fireblocks, accessed on April 11, 2025, https://www.fireblocks.com/blog/bybit-attack-security-flaws-fireblocks-nation-state-resilient-solutions/
49. Bybit Hack - Sophisticated Multi-Stage Attack Details Revealed - Cyber Security News, accessed on April 11, 2025, https://cybersecuritynews.com/bybit-hack-sophisticated-multi-stage-attack/
50. Bybit Hack Update: North Korea Moves to Next Stage of Laundering | TRM Blog, accessed on April 11, 2025, https://www.trmlabs.com/resources/blog/bybit-hack-update-north-korea-moves-to-next-stage-of-laundering
51. Bybit Incident Postmortem - blockscholes, accessed on April 11, 2025, https://www.blockscholes.com/research/bybit-incident-postmortem-how-bybit-rose-from-the-hack-and-protects-its-rpi-retail-users
52. Bybit's $1.4 Billion Hack: The Race to Recover Stolen Crypto from Lazarus Group, accessed on April 11, 2025, https://www.fintechweekly.com/magazine/articles/bybit-ceo-ben-zhou-says-most-funds-are-still-traceable
53. Breaking down the Bybit exchange hack - Crystal Intelligence, accessed on April 11, 2025, https://crystalintelligence.com/investigations/breaking-down-the-bybit-exchange-hack/
54. Bybit Confirms Record-Breaking $1.46 Billion Crypto Heist in Sophisticated Cold Wallet Attack - The Hacker News, accessed on April 11, 2025, https://thehackernews.com/2025/02/bybit-confirms-record-breaking-146.html?m=0
55. ByBit $1.5B Crypto Heist: ADR Best Practices and Lessons Learned | Oligo Security, accessed on April 11, 2025, https://www.oligo.security/blog/bybit-1-5b-crypto-heist-adr-best-practices-and-lessons-learned
56. What the Bybit Hack Means for Crypto Security and the Future of Multisig Protection, accessed on April 11, 2025, https://blog.checkpoint.com/security/what-the-bybit-hack-means-for-crypto-security-and-the-future-of-multisig-protection/
57. The need for enterprise security measures in the wake of the Bybit attack - Quant Network, accessed on April 11, 2025, https://quant.network/perspectives/the-need-for-enterprise-security-measures-in-the-wake-of-the-bybit-attack/
58. ByBit Billion Dollar Hack - Part 1: Smart Contracts Forensics Timeline - AnChain.AI, accessed on April 11, 2025, https://www.anchain.ai/blog/bybit

59. Bybit Suffers Historic $1.4 Billion Hack: A Blow to the Crypto Industry - IndraStra Global, accessed on April 11, 2025, https://www.indrastra.com/2025/02/bybit-suffers-historic-14-billion-hack.html
60. Crypto Theft Sees 303% Quarterly Jump After Record Bybit Hack - PYMNTS.com, accessed on April 11, 2025, https://www.pymnts.com/cryptocurrency/2025/crypto-theft-sees-303-percent-quarterly-jump-after-record-bybit-hack/
61. Bybit Hack by the Numbers - Kaiko - Research, accessed on April 11, 2025, https://research.kaiko.com/insights/bybit-hack-by-the-numbers
62. Hackers Steal Record $1.4 Billion from Bybit in Largest-Ever Crypto Heist - FinTech Weekly, accessed on April 11, 2025, https://www.fintechweekly.com/magazine/articles/bybit-hack
63. Bybit Hack Rattles Markets - NYDIG, accessed on April 11, 2025, https://www.nydig.com/research/bybit-hack-rattles-markets
64. Bybit Hack Postmortem - Glassnode Insights, accessed on April 11, 2025, https://insights.glassnode.com/the-week-onchain-week-08-2025/
65. Explained: The Bybit Hack (February 2025) - Halborn, accessed on April 11, 2025, https://www.halborn.com/blog/post/explained-the-bybit-hack-february-2025
66. The Bybit Incident: When Research Meets Reality - Check Point Research, accessed on April 11, 2025, https://research.checkpoint.com/2025/the-bybit-incident-when-research-meets-reality/
67. ByBit Hack: Exploiting Smart Contracts to Drain Funds - A Deep Dive on How it Happened, accessed on April 11, 2025, https://lukka.tech/bybit-hack-deep-dive/
68. Digital Assets Brief: Bybit Hack Underlines Importance Of Cyber Resilience - S&P Global, accessed on April 11, 2025, https://www.spglobal.com/ratings/en/research/articles/250225-digital-assets-brief-bybit-hack-underlines-importance-of-cyber-resilience-13426701
69. Most Secure Crypto Exchanges for 2025: How to Keep Your Investments Safe, accessed on April 11, 2025, https://coinmarketcap.com/academy/article/0679167d-8558-441b-96e8-8345794eff9e
70. Preventing Large-Scale Crypto Hacks: Key Security Measures for Exchanges - Chainalysis, accessed on April 11, 2025, https://www.chainalysis.com/blog/preventing-crypto-hacks-best-practices-for-exchanges-hexagate/
71. Lessons learned from the Bybit hack: A forensic accountant's perspective, accessed on April 11, 2025, https://www.grip.globalrelay.com/lessons-learned-from-the-bybit-hack-a-forensic-accountants-perspective/
72. Lessons from Bybit hack: How to stay safe on crypto exchanges - Cointelegraph, accessed on April 11, 2025, https://cointelegraph.com/learn/articles/lessons-from-bybit-hack-how-to-stay-safe
73. Bybit has lost $1.4 billion in a hack (Security lessons to learn) - QuillAudits,

accessed on April 11, 2025, https://www.quillaudits.com/blog/web3-security/bybit-hack-security-lesson
74. Lessons from the Bybit Hack: Rethinking Crypto Security - OneSafe Blog, accessed on April 11, 2025, https://www.onesafe.io/blog/bybit-hack-lessons-cryptocurrency-security-dea6b
75. The Bybit Hack: A Digital Asset Insurance Perspective and Lessons Learned - (Re)in Asia, accessed on April 11, 2025, https://reinasia.com/the-bybit-hack-a-digital-asset-insurance-perspective-and-lessons-learned/
76. The Bybit Hack: A crypto heist with cloud security lessons | SC Media, accessed on April 11, 2025, https://www.scworld.com/perspective/the-bybit-hack-a-crypto-heist-with-cloud-security-lessons
77. The $1.5B Bybit Hack: The Era of Operational Security Failures Has Arrived, accessed on April 11, 2025, https://blog.trailofbits.com/2025/02/21/the-1.5b-bybit-hack-the-era-of-operational-security-failures-has-arrived/
78. Bybit Opportunists: Malicious Infrastructure Attacks Report - BforeAI, accessed on April 11, 2025, https://bfore.ai/bybit-opportunists-malicious-infrastructure-attacks-report/
79. The Bybit $1.5B Hack: A Masterclass in Crisis Management - Kairon Labs, accessed on April 11, 2025, https://kaironlabs.com/blog/the-bybit-usd1-5b-hack-a-masterclass-in-crisis-management
80. The Bybit heist: how the hackers took control - Crystal Intelligence, accessed on April 11, 2025, https://crystalintelligence.com/investigations/the-bybit-heist-how-the-hackers-took-control/
81. TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies | CISA, accessed on April 11, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a
82. Incident Update: Unauthorized Activity Involving ETH Cold Wallet - Bybit Announcement, accessed on April 11, 2025, https://announcements.bybit.com/article/incident-update---eth-cold-wallet-incident-blt292c0454d26e9140/
83. Bybit Hack: SafeWallet Report Reveals Details of $1.4 Billion Cybersecurity Breach, accessed on April 11, 2025, https://www.binance.com/en/square/post/03-06-2025-bybit-hack-safewallet-report-reveals-details-of-1-4-billion-cybersecurity-breach-21195682977506
84. SafeWallet releases Bybit hack post-mortem report - TradingView, accessed on April 11, 2025, https://www.tradingview.com/news/cointelegraph:108027933094b:0-safewallet-releases-bybit-hack-post-mortem-report/
85. North Korea Responsible for $1.5 Billion Bybit Hack - Internet Crime Complaint Center, accessed on April 11, 2025, https://www.ic3.gov/PSA/2025/PSA250226

86. A race against time: How Elliptic's real-time intelligence is recovering funds from history's largest crypto hack, accessed on April 11, 2025, https://www.elliptic.co/blog/a-race-against-time-how-elliptics-real-time-intelligence-is-recovering-funds-from-historys-largest-crypto-hack
87. How to store cryptocurrency after the Bybit hack | Kaspersky official blog, accessed on April 11, 2025, https://www.kaspersky.com/blog/bybit-hack-lessons-how-to-do-self-custody-properly/53155/
88. Bybit Hack 2025: How to Keep Your Crypto Safe from Cyber Threats - Atomic Wallet, accessed on April 11, 2025, https://atomicwallet.io/academy/articles/bybit-hack-2025-how-to-keep-your-crypto-safe-from-cyber-threats
89. Explain me Bybit hack like I am 6 years old : r/ethereum - Reddit, accessed on April 11, 2025, https://www.reddit.com/r/ethereum/comments/1iw6jbn/explain_me_bybit_hack_like_i_am_6_years_old/
90. Safe Wallet releases update on $1.5b Bybit hack, lists new security enhancements - Mitrade, accessed on April 11, 2025, https://www.mitrade.com/insights/news/live-news/article-3-681193-20250307
91. February 28th, 2025: Statement by the Safe Ecosystem Foundation - Safe Global, accessed on April 11, 2025, https://safe.global/blog/safe-ecosystem-foundation-statement
92. A Safe-native Solution to the Bybit Hack - Ackee Blockchain, accessed on April 11, 2025, https://ackee.xyz/blog/a-safe-native-solution-to-the-bybit-hack/
93. What the Bybit Hack Reveals About Blockchain AML Weaknesses - Halborn, accessed on April 11, 2025, https://www.halborn.com/blog/post/what-the-bybit-hack-reveals-about-blockchain-aml-weaknesses
94. How Cobo Portal Enhances Safe{Wallet} Security Against Emerging Threats, accessed on April 11, 2025, https://www.cobo.com/post/from-threat-to-resilience-how-cobo-strengthens-safe-wallet-security
95. Bybit Confirms Security Integrity Amid Safe (Wallet) Incident - No Compromise in Infrastructure | Morningstar, accessed on April 11, 2025, https://www.morningstar.com/news/pr-newswire/20250226cn28105/bybit-confirms-security-integrity-amid-safe-wallet-incident-no-compromise-in-infrastructure
96. Bybit $1.4 Billion Breach Linked to Safe Wallet Vulnerability, Investigation Finds, accessed on April 11, 2025, https://www.financemagnates.com/cryptocurrency/bybit-14-billion-breach-linked-to-safe-wallet-vulnerability-investigation-finds/
97. How did Bybit hack 2025 happen: the full story - Techpoint Africa, accessed on April 11, 2025, https://techpoint.africa/guide/bybit-hack-2025/
98. Cobo at Cyberport 2025: Breaking Down the Bybit Breach and Wallet Security Lessons, accessed on April 11, 2025,

https://www.cobo.com/post/cobo-at-cyberport-2025-dissecting-the-bybit-breach-and-the-future-of-wallet-security
99. The Bybit Hack and the Future of Cybersecurity Compliance - USFCR Blog, accessed on April 11, 2025, https://blogs.usfcr.com/bybit-hack-cybersecurity-response
100. Bybit's Security Update: Asset Recovery and Enhanced Security Measure, accessed on April 11, 2025, https://announcements.bybit.com/article/bybit-s-security-update-asset-recovery-and-enhanced-security-measure-blt47be62971e11fb74/
101. The Bybit Heist: What Happened & What Now? | Wilson Center, accessed on April 11, 2025, https://mexicoelections.wilsoncenter.org/article/bybit-heist-what-happened-what-now
102. Safe Wallet Introduces New Security Features following Bybit Hack – Removes Ledger Integration - CoinStats, accessed on April 11, 2025, https://coinstats.app/news/d57851d1c3a40b3a9e682973fb3ac844ae7f0ad09e16727b3ce71ca9c6e31e98_Safe-Wallet-Introduces-New-Security-Features-following-Bybit-Hack--Removes-Ledger-Integration/
103. Top 9 Cryptocurrency Hardware Wallets for 2025 | Security Researcher Review, accessed on April 11, 2025, https://patrickalphac.medium.com/top-9-cryptocurrency-hardware-wallets-for-2025-security-researcher-review-9fcb16d771e0
104. Top Crypto Wallets of 2025: Balancing Security and Convenience - Hackread, accessed on April 11, 2025, https://hackread.com/crypto-wallets-2025-balancing-security-convenience/
105. Safe Wallet Review 2025: Pros, Cons, & Features - Milk Road, accessed on April 11, 2025, https://milkroad.com/reviews/safe-wallet/
106. Best Crypto Wallets for 2025: Security, Features, and Expert Recommendations - ECOS, accessed on April 11, 2025, https://ecos.am/en/blog/best-crypto-wallets-for-2025-security-features-and-expert-recommendations/
107. Safe wallet enhances security features after Bybit hack - Crypto News, accessed on April 11, 2025, https://crypto.news/safe-wallet-security-features-bybit-hack-2025/
108. Safe{Wallet} – Welcome, accessed on April 11, 2025, https://app.safe.global/
109. The Best Cold Storage Wallets 2025 - Safe.Global, accessed on April 11, 2025, https://safe.global/blog/best-cold-storage-wallets
110. Safe{Wallet} — Secure Smart Account Management on Ethereum, accessed on April 11, 2025, https://safe.global/wallet
111. 2025 Guide: What You Need to Know to Invest in Crypto Safely | Security.org, accessed on April 11, 2025, https://www.security.org/digital-security/crypto/
112. Cryptocurrency Transaction Monitoring: Best Practices in 2025 - FOCAL, accessed on April 11, 2025, https://www.getfocal.ai/blog/cryptocurrency-transaction-monitoring
113. Crypto Security in 2025 - How to Protect Your Crypto - Efani, accessed on

April 11, 2025, https://www.efani.com/blog/crypto-security
114. 2025 Crypto Policy Outlook | Grant Thornton, accessed on April 11, 2025, https://www.grantthornton.com/insights/articles/advisory/2025/crypto-policy-outlook
115. Preventing account takeover on centralized cryptocurrency exchanges in 2025, accessed on April 11, 2025, https://blog.trailofbits.com/2025/02/05/preventing-account-takeover-on-centralized-cryptocurrency-exchanges-in-2025/
116. Recent Developments Raise Significant Questions about the Future of Regulation and Enforcement of Cryptocurrency | Money Laundering Watch, accessed on April 11, 2025, https://www.moneylaunderingnews.com/2025/03/recent-developments-raise-significant-questions-about-the-future-of-regulation-and-enforcement-of-cryptocurrency/
117. Remote Code Execution via Man-in-the-Middle (and more) in NASA's AIT-Core v2.5.2, accessed on April 11, 2025, https://visionspace.com/remote-code-execution-via-man-in-the-middle-and-more-in-nasas-ait-core-v2-5-2/
118. Security Bulletin: Vulnerability in PyYAML affects IBM Spectrum Protect Plus Container and Microsoft File Systems Agents (CVE-2020-1747), accessed on April 11, 2025, https://www.ibm.com/support/pages/security-bulletin-vulnerability-pyyaml-affects-ibm-spectrum-protect-plus-container-and-microsoft-file-systems-agents-cve-2020-1747
119. CVE-2020-1747, accessed on April 11, 2025, https://www.cve.org/CVERecord?id=CVE-2020-1747
120. CVE - Search Results - MITRE Corporation, accessed on April 11, 2025, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=PyYAML
121. CVE-2020-1747, accessed on April 11, 2025, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1747
122. cve-2020-14343 - NVD, accessed on April 11, 2025, https://nvd.nist.gov/vuln/detail/cve-2020-14343
123. CVE-2020-14343 : A vulnerability was discovered in the PyYAML library in versions before 5.4, whe - CVE Details, accessed on April 11, 2025, https://www.cvedetails.com/cve/CVE-2020-14343/
124. Fully loaded: testing vulnerable PyYAML versions - Semgrep, accessed on April 11, 2025, https://semgrep.dev/blog/2022/testing-vulnerable-pyyaml-versions/
125. Improper Input Validation in PyYAML · CVE-2020-14343 · GitHub Advisory Database, accessed on April 11, 2025, https://github.com/advisories/GHSA-8q59-q68h-6hv4
126. CVE-2020-1747 Detail - NVD, accessed on April 11, 2025, https://nvd.nist.gov/vuln/detail/cve-2020-1747
127. cve-2020-1747 - NVD, accessed on April 11, 2025, https://nvd.nist.gov/vuln/detail/CVE-2020-1747
128. NVD Revamps Operations as Vulnerability Reporting Surges - Infosecurity

Magazine, accessed on April 11, 2025, https://www.infosecurity-magazine.com/news/nvd-revamps-operations-cve-surge/
129. Elliptic data used by US Secret Service in investigation into $96 billion Russian crypto exchange Garantex, accessed on April 11, 2025, https://www.elliptic.co/media-center/elliptic-data-used-by-us-secret-service-in-investigation-into-60-billion-russian-crypto-exchange-garantex
130. Bybit Exploit Blocklist - Elliptic Exploit API, accessed on April 11, 2025, https://www.elliptic.co/bybit-exploit-blocklist
131. Crypto exchange Bybit refills reserves after hackers steal a record $1.5 billion - YouTube, accessed on April 11, 2025, https://www.youtube.com/watch?v=LFs1-2y-qbw