Course Project – Cybersecurity Attack Analysis

Nemanja Milanovic

Old Dominion University

Susan Zehra

11/23/25

The Bybit Cryptocurrency Hack of 2025

Introduction

At the start of 2025, the cybersecurity environment saw a surge of attacks, never witnessed before in terms of frequency, sophistication, and worldwide consequences. Among the most fateful events that happened in this unstable environment was the hack of the Bybit cryptocurrency exchange in February 2025, where the hackers stole about half a million dollars, in the form of ETH, or about 500,000 ETH, worth about 1.4 billion US dollars. That event was not only one of the biggest thefts in the history of the digital world, but also a demonstration of some of the newer cybersecurity issues: involvement by nearly all countries, the use of cross-chain laundering, and the dynamic nature of digital asset infrastructure. The Global Cybersecurity Incident Review: January-April 2025 indicates that the attack was perpetrated by the North Korea-linked Lazarus Group, a threat actor that has been involved in significant financially based intrusions targeting cryptocurrency platforms on a large scale (Breached Company, 2025).

This paper also gives a detailed review of the Bybit hack, the context of the attack in the 2025 threat landscape, the technical and relaxing aspects of the attack, and the laundering process employed to cover up the stolen funds and the broader impacts of the hack on cybersecurity resilience in the cryptocurrency industry. It is aimed at providing a thorough knowledge of the attack and placing it in bigger trends that define digital security in 2025.

The 2025 Cybersecurity Environment

To analyze the Bybit hack in detail, one must consider more than just the cybersecurity climate where it took place. The period of four months in 2025 witnessed a spectacular increase in cyberattacks on organizations globally. The report by Breached Company indicated that organizations experienced 1,925 attacks a week on average, which is 47% higher in comparison to the timeframe in 2024 (2025). Ransomware has reached an unprecedented level, but significant instances of financial theft, in particular related to cryptocurrency, have grown as well.

Several reasons led to this escalation. To begin with, threat actors used more advanced social engineering methods, such as AI-assisted impersonation and deepfake-enhanced campaigns of vishing (Breached Company, 2025). Second, there has been a high shift in malware-free attacks whereby legit tools are abused in order to escape detection. Third, the presence of geopolitical tensions increased the activity of the nation-state groups against technology, finance, and government.

The Bybit breach was in line with these tendencies. It was consistent with the reported increase in state-centered attacks, particularly by North Korea, of digital setting assets to obtain revenue on behalf of legitimate regimes. The Bybit attack was one of the largest financial activities undertaken by the Lazarus Group, which was already attributed to several intrusions on cryptos.

Overview of the Bybit Hack

Initial Intrusion and Asset Theft

CoinDesk says that the breach at Bybit started when Lazarus agents acquired keys to one of its Ethereum cold wallets and sent all the ETH in the center to an anonymous account (Godbole, 2025). Although Bybit did not announce how the compromise happened, the scale of the incident strongly indicates that it was a targeted act and not a random adventure. Cold wallets are traditionally viewed as the most secure, as they are offline; therefore, it is probable that access to them requires privilege escalation via compromised internal credentials or a supply-chain or insider-related vector.

After gaining access to the wallet, the attackers used a rapid transaction with all the ETH before the security systems at Bybit could freeze the funds. Such urgent and complete extraction fits into the pattern of operation of the Lazarus Group. Previous cases indicate that Lazarus often conjures up asset drainage in one move before victims can react.

Attribution to the Lazarus Group

Blockchain forensic evidence, as well as behavioral indicators, confirm Attribution to the Lazarus Group. According to Breached Company (2025), Lazarus has taken on a particularly active role in early 2025 and increased its operations against exchanges and decentralized finance (DeFi) platforms. Historically, they have employed such laundering routes as mixers, cross-chain swaps, and fragmenting huge wallets. Also, the timing of the attack coincides with the financial requirements of North Korea, which is already subjected to international sanctions that have accelerated the action of Lazarus to choose more cyber-enabling revenue collection.

Laundering of the Stolen Funds

Among the most complicated aspects of the Bybit hack was the laundering plan to adopt and disguise the stolen cryptocurrency. The laundering phase also exhibited a high degree of operational planning and indicates more global changes in how illegal participants use blockchain infrastructure.

Use of Mixers to Obscure Transaction Trails

Bybit CEO Ben Zhou estimated that 27.95% of the money stolen was irreversible, as money that was stolen was sent through numerous layers of crypto mixers (Godbole, 2025). Wasabi, Railgun, Tornado Cash, and CryptoMixer are mixers that combine the income sources of a significant number of users to discontinue the trail of transaction history.

Mixers act as an anonymity layer that mixes several user inputs, redistributes the tokens in an unsystematic way, and practically disconnects the source and destination. Although there are valid privacy applications of mixers, they are often abused by threat agents since they make it hard to track them.

Cross-Chain Swaps and Bridges

The hackers also involved a complex system of bridges and cross-chain swap networks, such as Thorchain, eXch, Lombard, LiFi, Stargate, and SunSwap (Godbole, 2025). The services allow users to move assets among blockchains and add further complexity. One of the most challenging domains of inquiry continues to be cross-chain activity due to the presence of many protocols, liquidity pools, and decentralized structures, which are not always subject to the same regulatory measures by investigators.

One major revelation that was made by CoinDesk is that 84.45 percent of the stolen ETH, or more than 432,000 ETH, was sold to convert it into Bitcoin through Thorchain. This conversion is a classic Lazarus play converting volumes of ETH into BTC, which is more liquid, and they can distribute large volumes of assets over a large number of wallets, making it unnoticeable.

Wallet Fragmentation Strategy

The attackers then transferred the money to 35,772 wallets after conversion into Bitcoin, with an average of 0.28 BTC in each wallet (Godbole, 2025). This method is also typical of high-level laundering, as it is referred to as wallet shredding, or fragmentation. Dispersing funds in tens of thousands of small wallets, attackers lower the chances of being caught and further complicate tracking to an exponential scale.

This also allows the flexible liquidation using peer-to-peer (P2P) and over-the-counter (OTC) markets, where regulatory controls often are more lax. Zhou cites that one significant endpoint in the laundering chain was P2P and OTC channels (Godbole, 2025).

Frozen and Remaining Funds

Bybit and related exchanges had recovered or frozen only 3.84 percent of the money (Godbole, 2025). This minority percentage highlights how challenging it is to counter massive crypto theft when the attackers start the movement across their chains. Bybit found that 1.17% of stolen ETH was still on the Ethereum blockchain, spread over 12,490 wallets, which are the assets that were not yet fully laundered.

Security Weaknesses and Contributing Factors

Although Bybit did not provide detailed technical information about the breach, several factors can be deduced by using the known attack patterns and analysis of the industry.

Cold Wallet Mismanagement or Credential Exposure

The cracking of a cold wallet implies:

1. Privileged internal credentials were compromised,
2. An insider threat occurred,
3. Improper isolation of the cold wallet, or
4. A supply-chain vulnerability in the wallet management system.

Since Lazarus has been known to use spear-phishing and steal his credentials, a social engineering approach is viable. According to Breached Company (2025), in early 2025, there was a rise in advanced phishing schemes, including deepfake-assisted impersonation to gain access to employees.

Gaps in Monitoring of Cold Storage

Sometimes the cold wallets are perceived as necessarily safe, thus leading to slack patrol and a lack of an intrusion detection system. Without real-time warnings or multi-signature legislation, attackers were able to withdraw money without automatic protection in place on the cold wallet.

Cross-Chain and Mixer-Related Vulnerabilities

The speed with which money can be laundered by the attacker using the mixers and bridges points towards structural lapses throughout the cryptocurrency sector. Cross-chain tools have great ability and are usually not given standard security controls. This division forms vulnerabilities that other developed enemies can tap.

Broader Implications of the Bybit Hack

Growing Power of Nation-State Threat Actors

The extent and level of sophistication of the Bybit hack are indicative of the rising importance of nation-state actors in financially inclined Internet attacks. The participation of Lazarus Group is an example of the abuse of crypto platforms by state-aligned actors to serve a broader set of geopolitical ends. The effectiveness of this attack can encourage other actors supported by the state to use the same methods.

Urgent Need for Stronger Exchange Security Standards

No matter the fact that prominent exchanges are exposed to vulnerability, as seen in the incident. These areas need to be improved, and this includes:

- Wallet key management
- Multi-signature protections
- Cold wallet access controls

- Insider threat monitoring
- Real-time anomaly detection for large withdrawals
- Cross-chain transaction surveillance

Challenges of Regulating Cross-Chain Ecosystems

Regulators would have a big hurdle to jump since attackers had selected decentralized bridges and mixers. As detailed in the case, the following are required:

- Enhanced cooperation between exchanges
- Standardized reporting requirements
- Better blockchain analytics tools
- Global frameworks to address P2P and OTC off-ramps

Importance of Community-Driven Tracking

The work of Bybit called Lazarus Bounty, which was reported on more than 5,400 cases, demonstrates that the community's role in monitoring illegal crypto flows is becoming an even more significant one (Godbole, 2025). Cooperation between activities, users, and blockchain forensic specialists will be needed in the future.

Conclusion

One of the most notable cybersecurity events of the year is the Bybit hack of 2025 that influenced the industry financially, as well as allowed learning more about the emerging trends in terms of threats. The assault reveals the heightened level of professionalism of state-sponsored cybercrime, the weaknesses of cryptocurrency infrastructure, and the difficulty of locating cross-chain assets. In the larger scope of the growing cyber threat in the world, the Bybit breach is a wake-up call that even established, large-scale exchanges have to intensify their security measures.

With the ever-expanding digital asset sector, strong defenses, better regulatory collaboration, and more robust forensic tools will be necessary to avert such a wide-scale scenario in the coming years.

References

Company, B. (2025, April 22). *Global Cybersecurity Incident Review: January – April 2025*. Breached Company. https://breached.company/global-cybersecurity-incident-review-january-april-2025/

Godbole, O. (2025, April 21). *Bybit's CEO Ben Zhou Says Nearly 28% Funds From $1.4B Hack Have Gone Dark*. Coindesk.com; CoinDesk. https://www.coindesk.com/markets/2025/04/21/over-usd380m-worth-of-crypto-stolen-during-bybit-s-usd1-4b-hack-has-gone-dark