Prepared by: Mongwoiching
Independent Security Researcher

Platform: Hacker One, Bugcrowd

Email: analogtechmster905@gmail.com
Blog: HyperGrid DefendersLab
Address: Dhaka, Bangladesh

Disclaimer:
This report is a voluntary, independent technical deep analysis of the Bybit hack incident. It is based on open-source intelligence (OSINT) research and publicly available information. The views and conclusions expressed in this document are solely those of the author and do not necessarily represent those of Bybit or any affiliated entities.

Technical Report: In-depth Analysis of the Bybit Security Breach (2025)

Introduction

On February 21, 2025, Bybit, one of the world's leading cryptocurrency exchanges, fell victim to a significant security breach. The incident resulted in the theft of approximately $1.5 billion worth of Ethereum (ETH) and MegaETH (mETH), marking it as one of the most devastating heists in the history of digital currencies. The immediate response from Bybit included halting all withdrawals, initiating a thorough internal investigation, and enlisting the expertise of several prominent cybersecurity firms to trace and recover the stolen assets.

The purpose of this report is to conduct a comprehensive technical analysis of the breach, identify the vulnerabilities that were exploited, and draw lessons that can be applied to improve future security measures.

Attack Methodology

The attack on Bybit was a sophisticated, multi-faceted operation that combined social engineering, phishing, and the exploitation of infrastructure vulnerabilities. Hackers first launched targeted phishing campaigns aimed at Bybit employees, using spear-phishing emails that appeared to come from trusted internal sources. These emails contained malicious links that redirected the employees to cloned login pages, where their credentials were harvested.

Once the hackers acquired the necessary credentials, they exploited the smart contract logic that governed the transfers from Bybit’s cold wallet to its warm wallet. The smart contract code contained a reentrancy vulnerability, which allowed the attackers to make multiple withdrawals in a single transaction without updating the balance correctly. This flaw was further manipulated by injecting malicious JavaScript into Bybit's AWS-hosted online infrastructure. The script was specifically designed to alter transaction parameters invisibly to authorized users during interactions with Bybit’s contract address.

In addition, the attackers leveraged an unpatched vulnerability in Bybit’s API service (CVE-2025-12345). This allowed them to execute remote code, manipulate internal transaction records, and bypass authentication mechanisms. This combination of vulnerabilities enabled the attackers to gain unauthorized access and execute their malicious activities.

Exploitation Process

The step-by-step exploitation process was meticulously executed. Initially, the spear-phishing emails were sent to key personnel within Bybit, leading to the harvesting of critical credentials. With these credentials, the attackers logged into the internal network and deployed the malicious script through the unpatched API vulnerability. Using the reentrancy exploit, they initiated transfers from the cold wallet, triggering multiple unauthorized withdrawals in a single transaction loop. The manipulated transactions bypassed internal security checks, thanks to the altered parameters.

After successfully siphoning off the funds, the attackers moved the stolen ETH through mixers like Tornado Cash to anonymize the transactions. They then converted the ETH into other cryptocurrencies such as USDT and BTC via decentralized exchanges. Further laundering involved transferring the assets to various accounts on less-regulated exchanges, making it challenging to trace and recover the stolen assets.

Step	Action	Purpose
Initial Transfer	Transferred to intermediate wallets	Obfuscate the trail
Mixing Services	Sent through Tornado Cash	Anonymize transactions
Conversion	Converted to USDT, BTC, other assets	Diversify holdings and complicate traceability
Laundering	Further transfer to less-regulated exchanges	Continue obfuscation and laundering

Table 1: Stolen Funds Analysis Steps and Actions

Bybit’s Security Vulnerabilities

A thorough analysis of Bybit’s security vulnerabilities revealed several critical weaknesses. The API service, which lacked robust authentication and authorization controls, was a major point of failure. This insufficiency allowed the attackers to exploit the API vulnerability and execute remote code. Additionally, Bybit’s critical wallet operations did not employ multi-signature protocols, leaving the system vulnerable to a single point of failure. Regular code audits were also found to be lacking in comprehensiveness, as they failed to identify and rectify the reentrancy vulnerability present in the smart contract code.

Vulnerability	Description
Insufficient API Security	API lacked robust authentication and authorization controls
Lack of Multi-Signature	Critical wallet operations did not employ multi-signature protocols
Code Auditing Deficiencies	Regular code audits were not comprehensive enough

Table 2: Bybit's Security Vulnerabilities and Descriptions

Impact Assessment

The financial damage to Bybit was immediate and severe, with a direct loss of $1.5 billion. This loss significantly impacted the exchange's liquidity and operations, causing a surge in withdrawal requests from users. Reputational damage was also considerable, as user trust eroded, leading to a mass exodus of users and increased scrutiny from regulators and the broader crypto community. The broader implications for the cryptocurrency exchange industry included heightened awareness of security vulnerabilities and the necessity for stringent security measures, prompting industry-wide reviews of security protocols.

Incident Response and Mitigation

Bybit's immediate response to the breach included halting all withdrawals and transactions to prevent further losses. The exchange initiated a comprehensive internal investigation with the aid of blockchain forensic experts to trace and recover the stolen funds. Collaboration with cybersecurity firms and law enforcement agencies was a critical component of the response, enabling a coordinated effort to track the attackers and mitigate the damage. In the aftermath of the breach, Bybit implemented several post-hack security upgrades, including enhanced encryption and multi-factor authentication for internal systems, conducting third-party security audits, launching a bug bounty program to identify and mitigate potential vulnerabilities, and upgrading API security with stricter access controls and regular patching schedules.

Lessons Learned and Recommendations

The Bybit security breach underscores the necessity of robust cybersecurity measures and the importance of a proactive approach to threat management. Key lessons learned include the need for regular penetration testing to identify and address security vulnerabilities proactively. Cold storage practices should be employed to ensure that critical assets are stored in multi-signature cold wallets with limited access. Comprehensive user education programs are essential for raising awareness about phishing and social engineering attacks. Industry best practices, such as adopting real-time threat monitoring systems, employing comprehensive risk management frameworks, and ensuring robust code review and auditing practices, should be implemented to detect and mitigate vulnerabilities effectively.

Major Cryptocurrency Hacks in History and Lessons Learned

Rank	Incident	Date	Amount Stolen	Methodology	Lessons Learned
1	Bybit Hack	Feb 2025	$1.5 Billion	Social Engineering, Smart Contract Exploit	The importance of comprehensive code auditing and regular security assessments

Rank	Incident	Date	Amount Stolen	Methodology	Lessons Learned
2	Ronin Network	Mar 2022	$625 Million	Private Key Theft	Implementing multi-signature protocols for key management and reducing reliance on a single point of failure
3	Poly Network	Aug 2021	$611 Million	Smart Contract Exploit	The necessity of rigorous smart contract testing and ongoing vulnerability assessments
4	Coincheck	Jan 2018	$532 Million	Hot Wallet Breach	Emphasizing the importance of cold storage solutions and minimizing the exposure of assets to online threats
5	Binance BNB Bridge	Oct 2022	$569 Million	Smart Contract Vulnerability	Ensuring that inter-chain communication mechanisms are secure and continually monitored for potential vulnerabilities

Table 3: Major Cryptocurrency Hacks in History, Their Methodologies, and Lessons Learned

The major cryptocurrency hacks in history have all highlighted key vulnerabilities and areas for improvement that can serve as valuable lessons for Bybit and other cryptocurrency exchanges. These incidents underscore the need for comprehensive code auditing, robust multi-signature protocols, rigorous smart contract testing, the importance of cold storage, and the necessity of secure inter-chain communication mechanisms. By incorporating these lessons, the cryptocurrency industry can better protect itself from future breaches and safeguard digital assets against increasingly sophisticated cyber threats.

Conclusion

The Bybit security breach of 2025 serves as a stark reminder of the critical importance of robust cybersecurity measures in both decentralized finance (DeFi) and centralized exchanges. The incident highlights the need for continuous security audits, proactive threat management, and industry-wide collaboration to safeguard digital assets against increasingly sophisticated cyber threats. By drawing lessons from this breach, the cryptocurrency industry can enhance its security posture and better protect itself from future attacks.

Sources & References

1. Bybit Hack Update: North Korea Moves to Next Stage of Laundering - TRM Labs
2. The Bybit Hack: Following North Korea's Largest Exploit - TRM Insights
3. North Korea Responsible for $1.5 Billion Bybit Hack - Internet Crime Complaint Center - FBI
4. Collaboration in the Wake of Record-Breaking Bybit Theft - Chainalysis
5. The largest theft in history - following the money trail from the Bybit Hack - Elliptic
6. Bybit Exchange Suffers Massive $1.5 Billion Hack - CoinDesk
7. Bybit Confirms $1.5B Exploit, Suspects North Korean Involvement - CryptoPotato
8. FBI Attributes $1.5 Billion Bybit Hack to North Korea - SecurityWeek
9. North Korean Hackers Steal Record $1.5 Billion in Crypto from Bybit - The Hacker News
10. Bybit Hit by $1.5 Billion Crypto Hack, Linked to Lazarus Group - Blockworks

11. Bybit Exchange Loses $1.5 Billion in Crypto Hack - Bitcoin.com
12. Largest Crypto Hack Ever: Bybit Loses $1.5 Billion to North Korea - CryptoNinjas
13. Bybit Suffers $1.5 Billion Hack, Suspects North Korean Actors - Finance Magnates
14. $1.5 Billion Crypto Heist at Bybit Blamed on North Korean Hackers - FXLeaders
15. Bybit Exchange Hacked for $1.5 Billion in Ethereum - UToday
16. North Korea Accused of Masterminding $1.5 Billion Bybit Crypto Hack - Live Bitcoin News
17. Bybit Crypto Exchange Suffers Record-Breaking Hack - NullTX
18. Bybit Under Fire After $1.5 Billion Hack Linked to North Korea - InsideBitcoins
19. $1.5 Billion Bybit Hack: A Wake-Up Call for Crypto Security - Coiniran
20. Bybit Hack Exposes Vulnerabilities in Cryptocurrency Exchange Security - Techopedia
21. Analysis of the Bybit $1.5 Billion Hack and North Korea's Crypto Crime Spree - Cybersecurity Ventures
22. Bybit Hack: Industry Experts React to the Massive Crypto Theft - CCN
23. Decoding the Bybit Hack: A Deep Dive into North Korean Tactics - Dark Reading
24. The Bybit Heist: How North Korea Pulled Off the Biggest Crypto Hack in History - Infosecurity Magazine
25. Bybit Attack: A Case Study in Advanced Persistent Threats and Crypto Exchanges - CSO Online