Bybit Cryptocurrency Exchange Hack: Progress Report on Research

On February 21, 2025, Bybit, a prominent cryptocurrency exchange, faced a catastrophic security breach that resulted in the theft of approximately $1.5 billion worth of cryptocurrency assets. Among the stolen funds were 401,347 Ethereum tokens, making it the largest cryptocurrency theft in history. This incident surpassed previous high-profile breaches, such as the 2019 Binance hack ($546 million) and the 2022 Ronin Bridge exploit ($625 million).

Recent investigations have provided valuable insights into the attack's vector and methodology. Multiple intelligence agencies and blockchain security firms, including TRM Labs, Chainalysis, and the FBI, have attributed the breach to North Korea's notorious Lazarus Group. The FBI specifically identified a North Korean threat actor known as "TraderTraitor" as the perpetrator. This attribution aligns with North Korea's growing focus on cryptocurrency theft, as the Bybit hack alone surpassed all funds stolen by North Korean hackers in 2024.

The attack employed a sophisticated supply chain compromise targeting ***Safe{Wallet},*** a **multi-signature** wallet provider used by Bybit for cold storage management. On February 19, 2025, attackers compromised a Safe{Wallet} developer's machine through phishing, enabling them to replace a legitimate JavaScript file with malicious code on an AWS S3 bucket. This malicious code was designed to activate during the subsequent transaction, which occurred on February 21.

During what appeared to be a routine transfer from Bybit's Ethereum cold wallet to a hot wallet, the malicious code manipulated the transaction interface, displaying the correct destination address while altering the underlying smart contract logic. (More on this will be discussed in my presentation. The attack is far more sophisticated & ….ominous than implied here)

According to current reports, the attackers have nearly sold off all stolen ETH, leaving only approximately 60,000 ETH ($148 million) remaining to be laundered. Over the past 24 hours alone, the hackers have managed to launder 96,500 ETH, causing significant fluctuations in the Ethereum market. Prices plummeted to $2,440, resulting in a 2.8% decline within a single hour.

The Bybit hack represents a significant shift in cryptocurrency attack methodologies. Instead of directly exploiting vulnerabilities in blockchain protocols or smart contracts, the attackers targeted the user interface layer through a supply chain compromise. By injecting malicious code into Safe{Wallet}'s infrastructure, the hackers manipulated the signers' perceptions when approving transactions. This attack bypassed conventional security measures by exploiting "blind signing" – a vulnerability where signers approve transactions without fully comprehending their consequences – combined with a spoofed interface that closely resembled legitimate wallet software. This incident challenges conventional notions of cryptocurrency security, highlighting that despite robust smart contracts and multi-signature protections, the human-computer interface remains a critical vulnerability.

The latest developments as of March 1, 2025, indicate that the hackers have intensified their efforts to launder the stolen cryptocurrency. According to current reports, **roughly 90% of the illicit proceeds have been washed**, leaving only 60,000 ETH ($148 million) remaining to be laundered. Over the past 24 hours alone, the hackers have managed to launder 96,500 ETH, causing significant fluctuations in the Ethereum market. **Prices tumbled to $2,440, declining almost 3% in less than an hour.**

Evolution of Attack Methodology: Supply Chain Compromise and UI Manipulation

The Bybit hack represents a significant shift in cryptocurrency attack methodologies. Instead of directly exploiting vulnerabilities in blockchain protocols or smart contracts, the attackers targeted the user interface layer through a supply chain compromise. By injecting malicious code into Safe{Wallet}'s infrastructure, the hackers manipulated the signers' perceptions when approving transactions. This attack bypassed conventional security measures by exploiting "blind signing" – a vulnerability where signers approve transactions without fully comprehending their consequences – combined with a spoofed interface that closely resembled legitimate wallet software. This incident challenges conventional notions of cryptocurrency security, highlighting that despite robust smart contracts and multi-signature protections, the human-computer interface remains a critical vulnerability.

The Bybit hack, attributed to North Korean state-sponsored hackers, underscores the growing threat posed by nation-state actors in worldwide financial industry (**not** just crypto!) . According to TRM's 2025 Crypto Crime Report, North Korea was responsible for approximately $800 million in stolen cryptocurrency in 2024, accounting for about 35% of all stolen funds that year. This incident demonstrates a significant escalation in both the scale and sophistication of North Korean cryptocurrency operations, with striking similarities between the wallets used in this operation and those associated with past North Korean thefts.

The aftermath of the Bybit hack has caused substantial market disruption and prompted industry response. Bybit has initiated a bug bounty program, offering 5% of recovered funds to entities that assist in freezing assets and 5% to those who aid in tracing the funds. However, despite these efforts, only approximately 3% ($42 million) of the stolen cryptocurrency has been recovered, with some cryptocurrency services reportedly refusing to cooperate with recovery initiatives. The ongoing liquidation of stolen assets has led to significant market volatility, with Ethereum prices experiencing notable fluctuations. This incident has catalyzed renewed industry discussions about implementing more robust security measures. **It remains to be seen how this will affect the Trump administration's commitment to a BTC sovereign wealth fund.**

Presentation Outline

I. Introduction

- Overview of the Bybit cryptocurrency exchange
- Brief explanation of the hack: date, amount stolen, significance
- Thesis statement: The Bybit hack represents a watershed moment in cryptocurrency security, demonstrating new attack vectors, escalating state-sponsored threats, and challenging industry security assumptions

II. Technical Analysis of the Attack

- Timeline of events: from initial compromise to fund extraction
- Detailed breakdown of the attack methodology
    - Supply chain compromise of Safe{Wallet}
    - User interface manipulation
    - Exploitation of blind signing vulnerability
- Visual: Diagram showing the attack flow from phishing to fund extraction
- **Discussion Question 1: How might cryptocurrency exchanges better protect against supply chain attacks?**

III. Attribution and State-Sponsored Threats

- Evidence linking the attack to North Korean hackers
- Comparison with previous North Korean cryptocurrency operations
- Analysis of growing state-sponsored cryptocurrency theft trends

- Visual: Timeline showing escalation of North Korean cryptocurrency thefts
- **Discussion Question 2: What implications does state-sponsored cryptocurrency theft have for national security and international relations?**

IV. Market and Industry Impact

- Short-term market disruption and price effects
- Bybit's response and recovery efforts
- Industry-wide security reassessment
- Visual: Graph showing Ethereum price and trading volume fluctuations following the hack
- **Discussion Question 3: What security standards should be implemented industry-wide to prevent similar attacks?**

V. Lessons Learned and Future Implications

- Technical security recommendations
- Regulatory considerations
- Future trends in cryptocurrency security
- Visual: Security framework recommendation diagram
- **Discussion Question 4: How might this incident influence cryptocurrency regulation globally?**
-

VI. Conclusion

- Summary of key points
- Final thoughts on the significance of the incident
- Call to action for improved security practices

References

AnChain.AI. (2025, February 28). ByBit billion dollar hack - Part 1: Smart contracts forensics timeline. https://www.anchain.ai/blog/bybit

Barda, D., Ziakin, R., & Vanunu, O. (2025, February 27). The Bybit incident: When research meets reality. Check Point Research. https://research.checkpoint.com/2025/the-bybit-incident-when-research-meets-reality/

Chainalysis. (2025, February 24). Collaboration in the wake of record-breaking Bybit theft. https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/

Cointelegraph. (2025, February 21). 'Biggest crypto hack in history': Bybit exploit is latest security blow to industry. https://cointelegraph.com/news/biggest-crypto-hack-history-bybit-exploit-security-blo

Crystal Blockchain. (2025, February 25). Breaking down the Bybit exchange hack.

Elliptic. (2025, February 23). The largest theft in history - Following the money trail from the Bybit hack.

EmberCN. (2025, March 3). Bybit hacker's remaining 60000 ETH awaiting laundering. Blockchain News. https://blockchain.news/flashnews/bybit-hacker-s-remaining-60-000-eth-awaiting-laundering

Fireblocks. (2025, February 26). The flaw in "secure" systems: How ByBit's attack exploited blind trust.

Forbes. (2025, February 21). Latest on the Bybit record breaking 1.4 billion dollar crypto hack. https://www.forbes.com/sites/digital-assets/2025/02/21/latest-on-the-bybit-record-breaking-14-billion-dollar-crypto-hack/

Halborn. (2025, February 22). Explained: The Bybit hack (February 2025).

Ledger Insights. (2025, February 25). Bybit hack: phishing involved, plus how to prevent similar hacks.

NBC News. (2025, February 21). Hackers steal $1.5 billion from exchange Bybit in biggest-ever crypto heist. https://www.nbcnews.com/tech/crypto/hackers-steal-15-billion-exchange-bybit-biggest-ever-crypto-heist-rcna193273

SecurityWeek. (2025, February 27). FBI says North Korea hacked Bybit as details of $1.5B heist emerge. https://www.securityweek.com/fbi-says-north-korea-hacked-bybit-as-details-of-1-5b-heist-emerge/

SSRN. (2025, February 26). Crypto security in the aftermath of the Bybit hack: Evaluating risk management strategies for digital assets. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5156185

TRM Labs. (2025, February 27). The Bybit hack: Following North Korea's largest exploit. https://www.trmlabs.com/post/the-bybit-hack-following-north-koreas-largest-exploit

US Federal Contractor Registration. (2025, February 27). The Bybit hack and the future of cybersecurity compliance.