SYGNIA

BYBIT HEIST CASE STUDY:
WHEN BILLIONS VANISH: CYBER, FINANCE, AND GEOPOLITICS COLLIDE

On February 21, 2025, the cryptocurrency industry experienced what would become the largest documented digital asset heist in history. In a matter of minutes, approximately $1.5 billion worth of Ethereum—nearly 400,000 ETH—was siphoned from Bybit, one of the world's largest cryptocurrency exchanges.

What unfolded over the next several weeks revealed a sophisticated, multi-stage cyber operation involving social engineering, cloud compromise, web application tampering, and blockchain manipulation. More than a financial crime, the attack showed how cyber operations, global finance, and geopolitics are now tightly interwoven.

Company Background

Founded in 2018, Bybit has grown into the world's second-largest cryptocurrency exchange by trading volume, serving over 60 million active users globally. Headquartered in Dubai, with offices in Singapore, Hong Kong, and other jurisdictions, the company manages over $10 billion in assets across Bitcoin, Ethereum, USDT, Mantle, USDe, and other digital currencies.

Bybit employs approximately 1,500 people worldwide and runs complex custody mechanisms to safeguard client funds. Among these mechanisms are multi-signature (multi-sig) wallet configurations facilitated through Safe{Wallet}, a widely used non-custodial smart contract wallet running on Ethereum and other EVM blockchains.

Safe Smart Accounts are considered battle-tested infrastructure, with over 367 million total transactions, $100B+ in stored assets, and 43 million deployed accounts. Ironically, this trusted infrastructure became a principal part in the attack.

The Incident: February 21, 2025

On Friday, February 21, 2025, Bybit detected unauthorized activity involving its ETH cold wallets.

The malicious event occurred during what appeared to be a routine ETH multi-signature transaction facilitated through Safe{Wallet}. The transaction was intended to move assets from a cold wallet to a warm wallet. However, during the signing process, a threat actor manipulated the transaction payload.

Instead of executing the legitimate transfer, the attacker altered the transaction data while preserving the appearance of normalcy within the Safe{Wallet} interface. As a result, the authorized signers unknowingly approved a malicious transaction that granted the attacker control over the cold wallet.

Within minutes, approximately $1.5 billion USD worth of ETH was transferred to a wallet under the attacker's control .

The heist was complete.

Attack Timeline: A Multi-Stage Operation

Subsequent forensic investigation revealed that the February 21 theft was the culmination of nearly three weeks of preparation.[1]

PHASE 1: PREPARATION (FEBRUARY 2–4)

- **February 2, 2025:** The attacker registered the domain getstockprice[.]com, which would later serve as command-and-control (C2) infrastructure.
- **February 4, 2025:** A Safe{Wallet} developer's macOS workstation was compromised via social engineering. The lure delivered a malicious Python application that established initial access.

This marked the first foothold inside the broader environment.

PHASE 2: CLOUD INTRUSION & RECONNAISSANCE (FEBRUARY 5–17)

- **February 5:** Using stolen session tokens, the attacker accessed AWS resources and attempted to register a fraudulent MFA device.
- **February 5–17:** The attacker conducted extensive reconnaissance, enumerating IAM roles, S3 buckets, and other AWS resources.
- **February 17:** Command-and-control traffic within AWS indicated active attacker presence.

The adversary demonstrated patience and discipline, avoiding detection while mapping the cloud environment.

PHASE 3: WEB APPLICATION TAMPERING (FEBRUARY 19)

- **February 19:** Malicious JavaScript was injected into Safe{Wallet}'s frontend application hosted on AWS S3.

This step was pivotal. The injected JavaScript enabled the interception and manipulation of transaction data specifically targeting Bybit's transaction flows.

The attack did not aim to break cryptography or compromise private keys. Instead, it exploited trust in the user interface layer.

[1] https://x.com/safe/article/1897663514975649938/

PHASE 4: EXECUTION & CLEANUP (FEBRUARY 21)

- **February 21, 14:13 UTC:** The malicious transaction was executed, transferring approximately 400,000 ETH (~$1.5B).
- Immediately afterward, the attacker removed the injected JavaScript payload to erase evidence and complicate forensic analysis.

The entire blockchain component of the attack lasted minutes. The preparation lasted weeks.

The Technical Mechanism: Interface Manipulation

Forensic analysis found that the Safe{Wallet} frontend served altered JavaScript resources, including a modified _app-52c9031bfa03da47.js file.

Response headers and web archive comparisons confirmed that malicious code had been embedded into the JavaScript bundle. The injected logic changed transaction payload data in transit between user review and on-chain signing.

Critically, the Safe{Wallet} interface displayed legitimate transaction details to Bybit signers while malicious data was being signed and executed in the background.

This “display-sign mismatch” technique mirrors patterns seen in previous high-profile crypto thefts, including:

- **July 2024:** $230M loss
- **October 2024:** $50M loss

In those incidents, victims reported discrepancies between the transaction displayed in the interface and the one ultimately signed.

The Bybit case shows how UI-layer manipulation can defeat even multi-signature protection when trust in the interface is absolute.

Crisis Response & Industry Impact

IMMEDIATE COMMUNICATION

- **February 21, 15:44:** Bybit’s CEO announced the manipulated transaction on X.
- **February 21, 16:30:** Sygnia was engaged to help with the investigation.
- **February 21, 16:47:** Safe {Wallet} issued a first statement, saying there was no evidence of frontend compromise at that stage.
- **February 24:** Major investigative breakthrough found malicious injections to Safe{Wallet’s} website.

The Safe{Wallet} infrastructure was temporarily taken offline, affecting over $100B in assets under management. This action underscored the systemic implications of a compromise in shared Web3 infrastructure.

Behind the scenes, Bybit had to rapidly secure liquidity to ensure client withdrawals and keep market confidence. The exchange prioritized solvency transparency and operational continuity to prevent panic.

Attribution: The Geopolitical Dimension

The immediate suspect was the Lazarus Group, a North Korean state-linked threat actor known for large-scale cryptocurrency thefts.

North Korea has been linked to multiple sophisticated campaigns targeting DeFi platforms, exchanges, and blockchain infrastructure to fund its sanctioned regime. Billions in digital assets have been stolen to bypass international sanctions and finance weapons programs.

The Bybit attack aligns with Lazarus' historical tactics:

- Social engineering of developers
- Cloud token abuse
- Supply-chain compromise
- Strategic targeting of crypto custody infrastructure
- Rapid laundering of stolen digital assets

This case exemplifies how state-sponsored cybercrime can destabilize global financial platforms within hours.

Supply Chain & Third-Party Risk

Notably, investigation findings showed no evidence that prior heists directly originated from Safe{Wallet} infrastructure itself, and the earliest signs of developer workstation compromise occurred after earlier 2024 heists.

The broader lesson is not about a single vendor failure, but about systemic supply chain risk in Web3 ecosystems.

Crypto custody often depends on:

- Cloud infrastructure providers (AWS)
- Smart contract wallet platforms
- Frontend web applications
- Third-party libraries
- Developer endpoint security

When trust is layered across multiple parties, a single compromised link can cascade into billions in losses.

Key Insights & Lessons Learned

1. SOPHISTICATED, MULTI-STAGE CAMPAIGNS

This was not opportunistic hacking. It involved infrastructure registration, targeted social engineering, cloud reconnaissance, web tampering, and timed blockchain execution.

Modern adversaries operate like well-funded enterprises.

2. INTERFACE TRUST IS A CRITICAL VULNERABILITY

Multi-signature protections assume that signers see what they sign. When UI integrity is compromised, even secure cryptographic systems can be subverted.

3. SUPPLY CHAIN & THIRD-PARTY RISK ARE STRATEGIC THREATS

There is a lack of standardized security benchmarks across Web3 providers. Shared infrastructure amplifies blast radius.

4. HIGHLY MOTIVATED, ADAPTIVE ADVERSARIES

State-linked groups like Lazarus continuously refine tactics. Defensive strategies must evolve just as quickly.

Lessons in Effective Crisis Management

The Bybit heist is a strong example of high-stakes, real-time crisis management under extreme financial and reputational pressure. Stripping away the technical details, several clear lessons emerge about what worked—and what organizations should replicate.

1. COMMUNICATE FAST, EVEN IF THE INFORMATION IS INCOMPLETE

Bybit publicly acknowledged the incident before the root cause was known, sharing that an unauthorized transaction had occurred, an investigation was underway and committed to continued updates.

Early, transparent communication prevents speculation, reduces panic, and establishes control. Waiting for perfect information creates a vacuum others will fill.

2. PROTECT USERS AND MAINTAIN OPERATIONS AT ALL COSTS

Bybit never halted operations or user withdrawals. Doing so demonstrated liquidity and operational continuity in real time, reassuring users that their funds were safe.

Demonstrating that customer assets and core services remain secure is the single strongest trust signal. Continuity outweighs technical explanations in the early phase.

3. ANCHOR DECISION IN VALIDATED INTELLIGENCE

Bybit worked with incident response and blockchain experts ground their response and communications in verified findings. They built an accurate timeline of attack based on real facts, not false signals.

Translate complex technical events into what matters: impact, scope, and next steps. Clear framing reduces confusion and limits reputational fallout.

4. REINFORCE CREDIBILITY THROUGH THIRD PARTY VALIDATION

ByBit supported and enabled independent investigations by Sygnia and other security firms, sharing technical findings and root cause analysis.

Consistent post-incident updates and involvement of third-party experts strengthens trusts, demonstrates accountability and reinforces credibility.

Conclusion: A Defining Moment for Web3 Security

The Bybit heist was not merely the largest documented crypto theft—it was a defining moment for digital asset security.

It demonstrated:

- The fragility of trust in frontend interfaces
- The risks inherent in cloud-based Web3 infrastructure
- The scale of geopolitical motivations driving cybercrime
- The systemic interdependence of crypto ecosystems

When cyber, finance, and geopolitics blend into a single event, the consequences ripple far beyond the initial victim.

For exchanges, custodians, wallet providers, and regulators alike, the lesson is clear:

Security in Web3 is no longer just about private keys—it is about securing the entire operational, cloud, and supply chain ecosystem.

Continuous vigilance, proactive defense, transparent crisis management, and rigorous forensic investigation are no longer optional. They are existential requirements.

The events of February 21, 2025, will likely be studied for years—not only for the scale of loss, but for what they revealed about the future of cyber-enabled financial warfare.