Case Study: Bybit Cryptocurrency Exchange Hack

Prepared by: Rameen Mughal
Date: October 20, 2025

I. Case Summary

On February 21, 2025, Dubai-based crypto exchange Bybit suffered the largest crypto theft in history, losing around $1.5 billion in Ethereum (ETH) after hackers exploited vulnerabilities in its third-party wallet provider, Safe{Wallet}. The breach began when a Safe{Wallet} developer was deceived in a social engineering attack, allowing attackers to steal AWS session tokens and bypass MFA. With this access, they injected malicious JavaScript into the platform, secretly redirecting Bybit's transfers to North Korean-controlled addresses. The attack led to over $160 million laundered within 48 hours and triggered a 20% drop in Bitcoin's value, raising global concerns about crypto custody security.

II. Attack Vector

The Bybit hack began with a social engineering and supply chain attack targeting Safe{Wallet}, a third-party wallet service used by Bybit. According to Mandiant's investigation, the attackers posed as a trusted open-source contributor and tricked a Safe{Wallet} developer, one of the few with administrative access, into installing a malicious Docker Python project**.** This allowed the attackers to steal AWS session tokens**,** which are temporary security keys, and use them to bypass multi-factor authentication (MFA)**.** With these stolen tokens, the attackers gained full access to Safe{Wallet}'s internal systems.

After gaining access, the attackers modified the platform's web interface by inserting malicious JavaScript code**.** This code secretly changed the destination of Ethereum (ETH) transfers from Bybit's wallets to wallets controlled by North Korean hackers**.** The attack was carefully planned to affect only Bybit's transactions, showing it was a highly targeted and well-coordinated operation**.** This combination of social engineering, supply chain compromise, and system manipulation led to one of the largest cryptocurrency thefts in history.

III. CIA Analysis

The Bybit hack compromised all three elements of the CIA triad — Confidentiality, Integrity, and Availability, to different degrees.

- **Confidentiality** was breached when the attackers gained unauthorized access to Safe{Wallet}'s internal systems by stealing AWS session tokens. This gave them access to sensitive credentials, internal scripts, and transaction data that should have remained private.

- **Integrity** suffered the most damage in this incident. The attackers modified Safe{Wallet}'s user interface and replaced legitimate JavaScript code with malicious code that secretly redirected Ethereum transfers. This manipulation altered the intended behavior of the system, violating data and transaction accuracy which is a direct compromise of integrity.

- **Availability** was also indirectly affected. After the breach, Bybit had to suspend operations temporarily to investigate and secure its systems. This caused downtime for users and disrupted normal transaction activities, impacting the platform's reliability and accessibility.

IV. Security Domains Involved

Several key security domains failed during the Bybit breach, contributing to the scale of the attack.

- First, the **Access Control** domain was compromised when the attackers stole AWS session tokens and bypassed multi-factor authentication (MFA). This allowed them to gain unauthorized administrative access to Safe{Wallet}'s systems without proper verification or detection.

- Secondly, the **Software Supply Chain Security** domain also failed, as the attackers successfully introduced malicious code through a compromised open-source project. This highlighted weak vetting and monitoring of third-party dependencies and developer tools.

- Finally, **Network and Cloud Security** controls were not strong enough to detect or block suspicious activity within the AWS environment, allowing the attackers to remain hidden until the funds were transferred.

V. Mitigation & Response

- **Immediate Incident Response:** Bybit and Safe{Wallet} quickly halted all ongoing transactions and transfers to prevent further losses once the breach was discovered. A full system lockdown was initiated to isolate compromised environments.

- **Forensic Investigation:** Cybersecurity firm Mandiant was brought in to investigate the breach, trace the attack path, and identify the methods used by the North Korean threat actors.

- **User Communication & Transparency:** Bybit publicly acknowledged the incident and assured users that they were working to recover lost funds and enhance platform security.

- **System Hardening:** Bybit and Safe{Wallet} strengthened their login security, checked and limited who had access to important systems, and changed all AWS credentials to make sure attackers couldn't get back in.

- **Improved Supply Chain & Developer Security:** The organizations introduced stricter code review policies, enhanced monitoring of third-party integrations, and increased developer training on social engineering and open-source trust verification.

VI. Lessons Learned

The following are the preventive measures that could have been taken and the organizations can adopt to avoid similar incidents in the future:

- **Strengthen Developer Awareness:** Developers should receive regular training to recognize social engineering and phishing attempts, especially those involving open-source collaborations or code contributions.

- **Secure Software Supply Chain:** All third-party and open-source tools should be carefully reviewed and verified before use. Automated dependency scanning and code-signing can help detect and block malicious components early.

- **Enhance Access Control and Authentication:** Implement stricter access management by enforcing short-lived credentials, strong MFA, and regular monitoring of privileged accounts.

- **Regular Security Audits:** Conducting frequent audits and penetration testing can reveal weaknesses in authentication, access control, and software handling processes.

VII. Key Terms and Definitions

- **Cold Wallet:** An offline cryptocurrency wallet used for long-term storage, offering high security against online threats.

- **Warm Wallet:** A wallet connected to the internet but with more security than a hot wallet, used for quicker access to funds.

- **AWS Session Tokens:** Temporary credentials that grant access to cloud resources on Amazon Web Services (AWS).

- **Social Engineering:** A manipulation technique that tricks individuals into revealing confidential information or performing risky actions.

- **Supply Chain Attack:** A cyberattack targeting third-party vendors or developers to compromise a larger organization indirectly.

- **Multi-Factor Authentication (MFA):** A security process requiring two or more verification methods to access a system.

- **Cryptocurrency:** A digital form of money that uses encryption to secure transactions and operates independently of traditional banks or governments.

- **Ethereum (ETH):** A popular blockchain-based cryptocurrency that allows not only digital payments but also supports smart contracts — self-executing agreements written in code.

VIII. Conclusion

The Bybit hack of February 2025 highlights how one weak link in this case, a compromised developer and poor supply chain security can lead to massive losses. It shows that technical defenses alone are not enough without strong awareness, access control, and monitoring. Bybit's quick response and transparency were important steps toward recovery, but the incident reminds all organizations to stay proactive, secure their supply chains, and strengthen overall cyber resilience.

IX. References

- The bybit heist: What happened & what now? (2025, March 31). Wilson Center.
- Rajic, T., & Brock, J. (2025, March 28). The ByBit Heist and the Future of U.S. Crypto Regulation.
- Kaminsky, S., & Kaminsky, S. (2025, March 17). Lessons from the Bybit hack: how to store crypto safely. *Kaspersky Official Blog*.