[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/who-is-lazarus-group-unraveling-the-mystery-behind-bybits-1-4b-hack

Who Is Lazarus Group: Unraveling the Mystery Behind Bybit's $1.4B Hack

On February 21, 2025, a $1.4 billion breach rocked Bybit, one of the leading cryptocurrency exchanges, shocking the whole crypto industry. Just a day after the attack was revealed, blockchain investigator ZachXBT shared findings that linked the hack to the DPRK-backed hacking group.

Regarded as the largest cryptocurrency heist in history, this breach has once again brought the elusive Lazarus Group into the spotlight. So, who exactly are these cyber criminals, and how did they manage to steal such a staggering sum? Let's delve into the mystery behind Bybit's hack and uncover the secrets of this notorious group.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

Bybit Hack: A Masterclass in Cybercrime

The Bybit hack unfolded with unsettling precision. On February 22, 2025, Bybit officially reported the attack on its Announcement page, revealing that on February 21 at approximately 12:30 PM UTC, unauthorized activity had been detected in one of their Ethereum (ETH) Cold Wallets during a routine transfer.

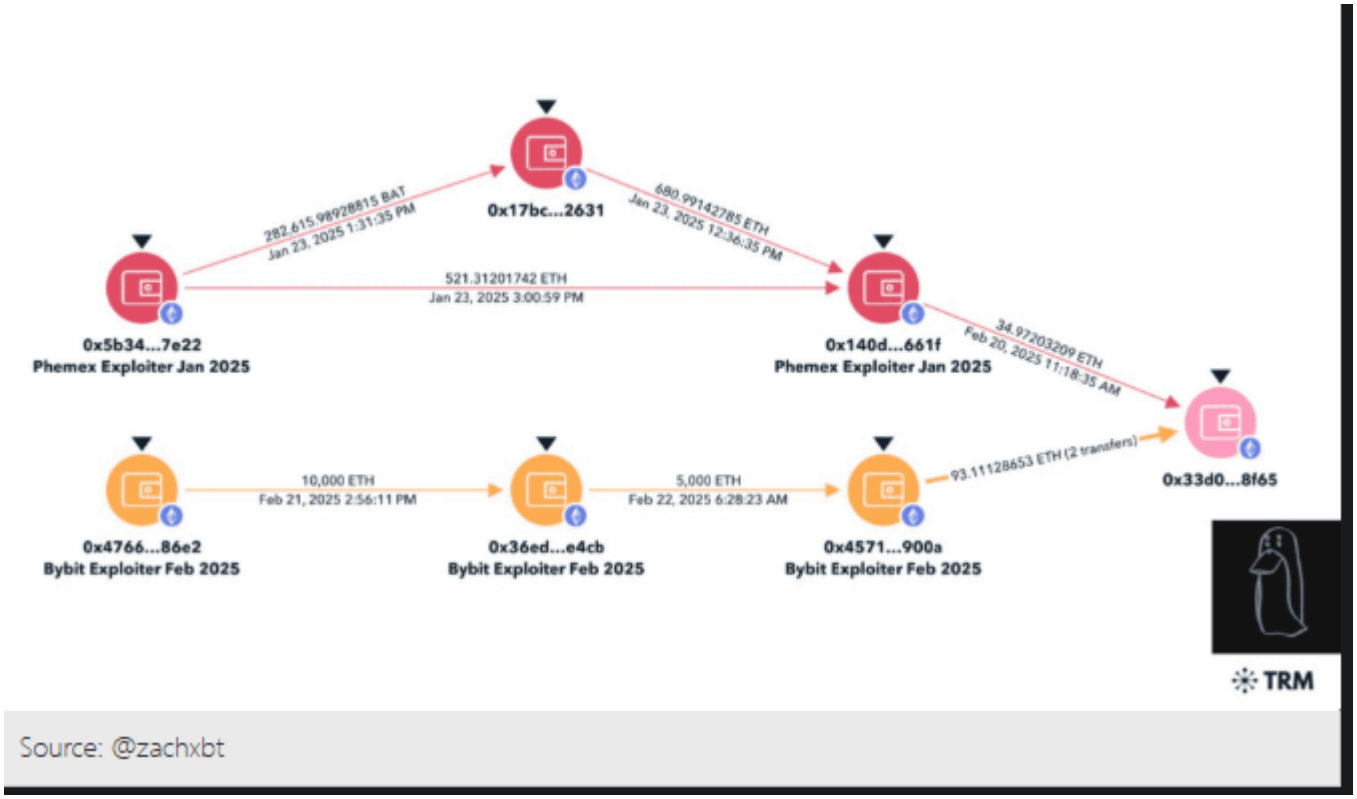
Despite being marketed as a highly secure offline storage solution, Bybit's Ethereum cold wallet was compromised while transferring funds to a warm wallet. The attackers cleverly disguised their malicious transaction as legitimate by modifying the smart contract rules, ultimately gaining control over the wallet.

Bybit confirmed that over 400,000 ETH and stETH, worth more than $1.5 billion, were transferred to an unidentified address. Following the breach, the exchange reported processing 70% of withdrawal requests, which likely surged after the hack was confirmed.

Bybit CEO Ben Zhou promptly reassured users that the exchange remained solvent and that all customer funds were fully backed on a 1:1 basis. However, the damage had been done—both financially and to the credibility of the broader crypto sector.

ZachXBT, a famous blockchain investigator, solved the case thoroughly, providing a comprehensive breakdown of the attack. Through trial transactions, wallet associations, and forensic timestamps, he

linked the theft to the Lazarus Group, a notorious hacking collective with a history of disrupting the crypto space.



ZachXBT also discovered that addresses tied to previous hacks, such as those involving Phemex and BingX, were linked to the same cluster associated with the Bybit breach.

“I spent the entire day graphing out the laundering movements and flagged theft addresses,” ZachXBT said while sharing the addresses connected to the Bybit hack.

Within hours, Arkham Intelligence—which had placed a $50,000 reward for information on the attackers—validated ZachXBT’s findings, confirming the Lazarus Group as the perpetrators behind this extraordinary heist.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

Who is the Lazarus Group?

The Lazarus Group, also known as APT38, is a cyber espionage collective that has been active since at least 2009. Believed to be based in North Korea, the group is closely tied to the country's Reconnaissance General Bureau, an intelligence agency. Over the years, Lazarus has targeted a wide range of industries, including banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs across at least 38 countries, employing sophisticated cross-platform attacks.

Since its emergence around 2007, the group has honed its skills over nearly two decades, blending espionage, financial theft, and creating global chaos. Nicknames like APT38 and TraderTraitor only hint at their operation. The Lazarus Group has evolved significantly, with a marked increase in both the sophistication of their tactics and the scale of their operations.

Their track record reads like a cyber-thriller. One of their earliest known attacks, "Operation Troy" (2009–2012), was a cyber-espionage campaign that targeted the South Korean government in Seoul. The group used relatively simple DDoS (Distributed Denial of Service) techniques to disrupt government systems.

However, their activities escalated dramatically in the following years. In 2016, the Lazarus Group was responsible for the infamous Bangladesh Bank heist, where they successfully stole $81 million. In 2017, they struck again, this time targeting the Far Eastern International Bank of Taiwan, stealing $60 million, though a large portion of the funds was later recovered.

In the world of cryptocurrency, Lazarus has become notorious for their high-profile heists, accumulating billions in stolen assets. Notable incidents include:

- **Ronin Network Heist (March 2022)**: The group stole $620 millionfrom the Axie Infinity blockchain, one of the largest thefts in crypto history.
- **Horizon Bridge Raid (June 2022)**: Lazarus lifted $100 millionfrom Harmony's cross-chain bridge.
- **Phemex Exchange Breach (January 2025)**: The group successfully stole over $70 millionfrom Singapore's Phemex exchange, following their typical modus operandi.

The Bybit hack in February 2025—which saw the Lazarus Group secure 500,000 ETH—solidified their position as one of the largest holders of Ethereum globally, surpassing even Vitalik Buterin. This haul catapulted them to become the 14th largest Ether holder in the world. These attacks underscore Lazarus' evolving strategies and their ability to exploit vulnerabilities in the cryptocurrency sector, continuously adapting to outsmart their targets.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

How does Lazarus Group Operate?

The Lazarus Group is infamous for its ability to adapt and evolve, continuously refining its tactics and expanding its range of tools, making it one of the most formidable cybersecurity threats in the world. Over the years, the group has orchestrated a variety of operations—most of which involve disruption, sabotage, financial theft, and espionage.

Their playbook is as sophisticated as it is ruthless. The Lazarus Group employs custom malware, such as Manuscrypt, AppleJeus, and FALLCHILL, to infiltrate systems. Phishing attacks are their specialty, often executed through fake LinkedIn profiles or spear-phishing emails that deceive employees into revealing their login credentials.

The Bybit hack showcased their latest trick: "blind signing". This technique involves crafting a legitimate-looking user interface that hides a malicious payload, making it nearly impossible for the victim to detect the attack until it's too late. The group has also perfected the art of social engineering, using tactics like fake job offers, as seen in the 2023 CoinsPaid breach, to lure victims into compromising their systems.

Once inside, the Lazarus Group moves quickly. Stolen funds are immediately dispersed across multiple wallets, laundered through DeFi platforms like Uniswap (which doesn't require KYC), and further obscured by using mixers. In the case of the Bybit breach, the stolen 500,000 ETH was tracked across 53 different wallets, showcasing the group's skill in evading detection and disappearing into the depths of the blockchain. However, dumping such a massive amount of Ethereum in a bearish market could prove to be a challenge, even for the Lazarus Group.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

What can we Learn from Bybit Hack?

The Bybit breach isn't just another headline—it's a critical wake-up call. The Lazarus Group's relentless attacks have exposed glaring vulnerabilities in even the most fortified crypto platforms. For Bybit users in Singapore and beyond, it serves as a harsh reminder: not your keys, not your coins.

While CEO Ben Zhou's pledge to cover the losses provides some reassurance, bolstered by the exchange's $20 billion in assets, the aftermath was still significant. The Ethereum price took a notable hit, dropping 8% in the wake of the hack.

But this attack isn't just the work of random criminals—it's part of a larger state-backed operation. The U.S. government estimates that North Korea's crypto thefts fund up to 30% of its missile program, turning digital wallets into weapons of geopolitical power.

Thanks to the rapid efforts of ZachXBT, alongside the work of firms like Elliptic and Chainalysis, the industry's response is beginning to gain traction. However, recovering from a breach of this scale remains a formidable challenge, especially when facing a nation-state adversary like the Lazarus Group.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

Conclusion

The Lazarus Group's $1.4 billion Bybit heist is not just a record-breaking theft—it's a chilling look into a shadowy conflict where cybercrime meets geopolitics. Uncovered through ZachXBT's investigation, these North Korean hackers remain a formidable force, blending advanced technological expertise with state-backed audacity. As the cryptocurrency market expands, so does their influence. This highlights the urgent need for exchanges and custodial providers to bolster their security measures and better protect user funds.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

About BTCC

Fully licensed and regulated in the **U.S., Canada, and Europe**, BTCC is a well-known cryptocurrency exchange, boasting an impeccable security track record since its establishment in 2011, with **zero reported hacks or breaches**. BTCC platform provides a diverse range of trading features, including **demo trading, crypto copy trading, spot trading,** as well as **crypto futures trading** with a leverage of up to **500x**. If you want to engage in cryptocurrency trading, you can start by signing up for BTCC.

BTCC is among the best and safest platforms to trade cryptos in the world. The reasons why we introduce BTCC for you summarize as below:

Industry-leading security

BTCC attaches great importance on security. Since founded in 2011, BTCC has never been hacked or been a victim of any other kind of successful malicious attack, which fully illustrates its security capabilities. Through measures like segregation of assets, 1:1 storage of users' assets, money laundering prevention and identity authentication and no collateralising tokens for loans, BTCC enjoys good reputation in asset security.

High Liquidity & Volume

BTCC is ranked top 10 by trading volume on both CoinMarketCap and CoinGecko, the world's two largest crypto information platforms. BTCC prides itself on providing crypto futures trading services to users worldwide with market-leading liquidity, offering perpetual futures on over 300 cryptocurrencies, including BTC, ETH, DOGE, LTC, SOL, XRP, SHIB, etc.

Extremely low fees

Charging high fees means less return for investors. Compared with other major exchanges, BTCC only charges 0.06% for both takers and makers, which are far below the industry average. According to the largest and most recent empirical study on crypto exchange trading fees, the average spot trading taker fee is 0.2294% and the maker fee is 0.1854%.

High and rich bonus

BTCC holds all kinds of campaigns where investors can participate to win exciting bonus. For example, new users can get rewards up to 10,055 USDT coupon through completing relevant missions, like registration, identity verification, first deposits, cumulative futures trading volume, etc. Besides, becoming VIP also can enjoy rewards like VIP-exclusive perks, including discounts on

trading fees, access to exclusive campaigns, BTCC merch, priority customer support, fast withdrawal, and many more.

Excellent customer service

BTCC also gains great reputation in terms of customer support. If you are confused or have problem in the process of trading currencies, you can obtain customer support via email and live chat, BTCC offers 24/7 online customer service for you.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

You May Like:

BTCC Exchange Review 2025

Bybit Hack: Everything You Need To Know About It

8 Types of Crypto Scams to Avoid in 2025

Best Non KYC Crypto Exchanges In February 2025

Understanding KYC In Crypto: How To Complete KYC On BTCC

What Is Spot Trading In Crypto & How To Start Crypto Spot Trading On BTCC: A Comprehensive Guide For 2025

A Beginner’s Guide: What Is Copy Trading & How To Start Copy Trading On BTCC

Best Crypto Exchanges Australia 2025

Pi’s Open Mainnet Goes Live On February 20: Everything You Need To Know About It

How To Buy Pi Network (PI): A Comprehensive Guide In 2025

Pi Network Mainnet Launch Now Goes Live: Pi Network Price Prediction Post Mainnet Launch

Pi Network (PI) Price Prediction: Will Pi Coin Reach $500 After Major Exchange Listings?

How to Sell Pi Coin in Canada: A Complete Guide for 2025

What Is Pi Network Dog (PIDOG) Meme Coin: PIDOG Rides High As PI Mainnet Introduces It In First 20 Apps

Mutuum Finance (MUTM) Coin Review & Analysis: Next 100x Gem?

What Is DeepSeek? Everything You Need To Know About It

Official TRUMP ($TRUMP) Price Prediction: Next 100X Trump-Themed Meme Coin?

Melania Meme ($MELANIA) Coin Review & Analysis: Melania Trump launches Her Own Meme Coin $MELANIA

BeerBear (BEAR) Meme Coin Review & Analysis: 100X Meme Coin On Solana?

The Last Dwarfs ($TLD) Meme Coin Review & Analysis: Next 100X Meme Coin?

BTCC vs. Kraken

BTCC vs. Coinbase vs. Crypto.com

Compare BTCC vs. Binance: Which is a Better Choice for Canadian Traders in 2025?

Compare BTCC vs. BitMart 2024: Which is a Better Choice for Your Demand

Compare BTCC vs Gate.io: Which is Best in 2025

BTCC vs CoinJar: Which One is Better?

BTCC vs. MEXC: A Complete Comparison In 2025

BTCC vs. Bitbuy

BTCC vs. NDAX: which is a better choice for crypto trading in Canada?