Immunefi

# LAZARUS GROUP REPORT

PREPARED BY IMMUNEFI

# Lazarus Group Report

PREPARED BY IMMUNEFI

The team at Immunefi, the leading bug bounty and security services platform for web3 which protects over $60 billion in user funds, has assessed the volume of crypto funds lost due to the attacks of the Lazarus Group, a North Korea-affiliated hacker group.

## OVERVIEW

The global web3 space was valued at over **$934 billion** in 2022. That capital represents an unparalleled and attractive opportunity for blackhat hackers.

We have reviewed instances where the Lazarus Group hackers have allegedly attacked various crypto projects. We have located 10 such cases across both DeFi and CeFi.

In total, we have seen a loss of **$1,903,600,000** across the web3 ecosystem from 2021 to 2023, due to the Lazarus Group. **$308,600,000** was stolen in CeFi across 5 specific incidents, and **$1,595,000,000** was stolen in DeFi across 5 specific incidents. Most of the sum came from the attack on Axie Infinity's Ronin Network, which resulted in a loss of $650,000,000, and Poly Network, which suffered a $600,000,000 loss.

In 2023, the group was allegedly behind the high-profile attacks on Atomic Wallet, CoinEx, Alphapo, Stake, and CoinsPaid, which collectively lost a staggering total of **$308.6 million** between June and September.

# Lazarus Group

A transition to crypto-focused attacks that is paying off.

## $1.9 billion

Stolen from web3 projects between 2021 and 2023.

## $625 million

Stolen from Axie Infinity’s Ronin Network in Lazarus' largest attack.

## $308.6 million

Stolen from web3 projects in 5 successful attacks in 2023.

# Lazarus Group

## LAZARUS GROUP AND THE FIRST NOTORIOUS ATTACKS

Lazarus Group is a North Korean-based hacker group responsible for some of the largest cyber attacks worldwide between 2010 and 2023. The group consists of an unknown number of individuals and is affiliated with the government of North Korea.

While the group's earliest known attack occurred between 2009 and 2012, in which it targeted the South Korean government with a cyber-espionage campaign that also utilized distributed denial-of-service attack (DDoS) techniques, they only achieved widespread attention after 2014.

Lazarus gained significant notoriety following the attack on Sony Pictures in 2014 and the cyber heist on the Central Bank of Bangladesh in 2016, which led to $81 million in losses. The group was also responsible for the worldwide spread of the infamous WannaCry ransomware in 2017, which encrypted victims' files for a ransom demand of $300-$600 in Bitcoin, in order for their data to be unlocked. WannaCry stands as one of the first notable global ransomware attacks. Within hours, it spread and infected approximately 230,000 computers across 150 countries.

## DEDICATED TRAINING

North Korean hackers undergo specialized training in Shenyang, China, where they receive instruction on how to deploy various forms of malware across computers, networks, and servers. Within North Korea, their education begins at institutions like the Kim Chaek University of Technology, Kim Il-sung University, and Moranbong University. These universities selectively admit the most talented students nationwide, providing them with six years of rigorous and specialized education in this field.

# Lazarus Group

## BRIDGING WEB2 AND WEB3

Lazarus predominantly focuses on cybercrime activities that yield immediate financial gains. Its expansion into cryptocurrency attacks since 2017 comes as a natural evolution. Unlike regular software, the web3 industry is unique because vulnerabilities in smart contracts represent the possibility of a direct loss of funds. With web3, billions of dollars in user funds are locked in permissionless smart contracts. Though significant skill is required, anyone can study those contracts, find an exploit, and leverage it directly to steal funds.

Furthermore, by moving into blockchain technology, Lazarus is able to sidestep international financial sanctions and use sophisticated money laundering schemes. They use mixers or tumblers such as Tornado Cash that obscure the destination of their illicit funds.

This makes web3 the perfect playground for an organization such as Lazarus.

The Lazarus Group carried out attacks on Bitcoin and Monero users, primarily in South Korea. These attacks mirrored prior incidents involving WannaCry ransomware and the Sony Pictures breach. Other tactics included spear-phishing emails loaded with malware, targeting users of cryptocurrency exchanges like Coinlink to pilfer email credentials and passwords.

During February 2017, attackers siphoned off $7 million from Bithumb, a South Korean exchange. Following cyberattacks in April and December 2017, Youbit, another South Korean Bitcoin exchange, declared bankruptcy. In December 2017, Nicehash, a marketplace for cryptocurrency cloud mining, encountered a loss of over 4,500 Bitcoin. Ongoing investigations indicated a connection to the Lazarus Group, further solidifying their involvement in the widespread breaches.

# Lazarus Group

## INFRASTRUCTURE VS. SMART CONTRACTS

A recent report from Immunefi reveals that **nearly half (46.5%)** of the funds lost in web3 result from traditional web2 security issues related to infrastructure (negligent private key management, weak passphrases, lack of firewalls, etc.), rather than smart contracts.

Web3 might be decentralized in some ways, but projects and users still control the keys to their wallets and run software on cloud computing services such as AWS. Exposure of this infrastructure leads to hacks and losses, even though the smart contract itself may be well-written, designed, and tested.

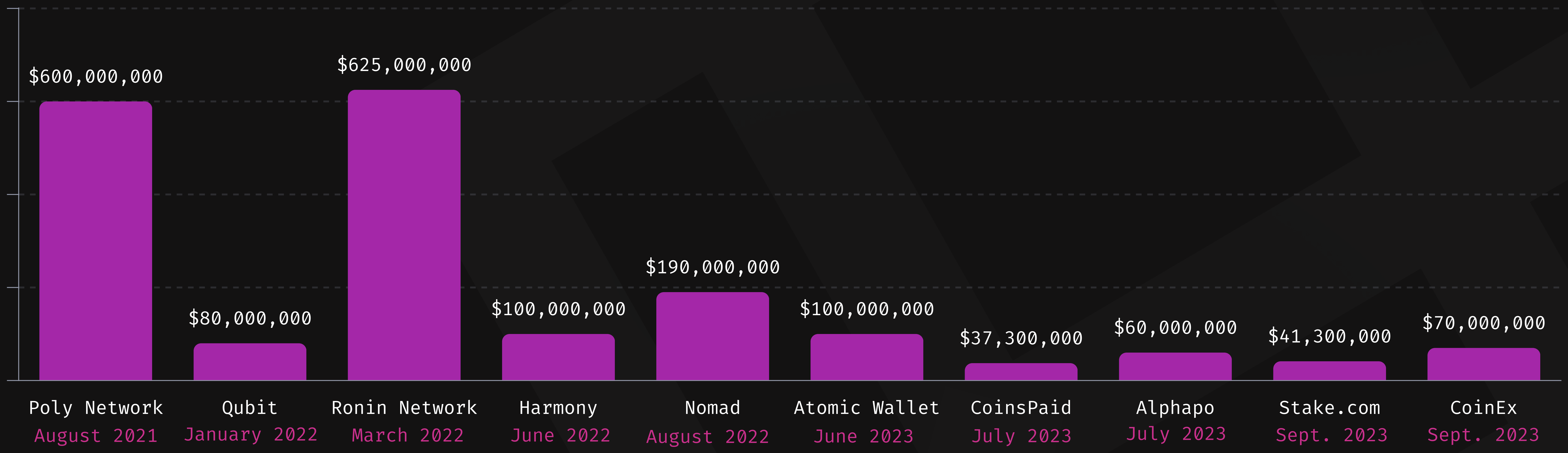
In 2023, web3 losses have primarily been driven by large-scale exploits, with a growing influence of state-backed actors such as Lazarus Group. These actors leverage their expertise to exploit traditional vectors such as the ones mentioned above to employ sophisticated attacks.

Looking ahead into 2024, it's evident that the Lazarus Group has notably elevated its sophistication, emerging as a significant threat to web3. Their proficiency in targeting this ecosystem has grown substantially, exploiting infrastructure vulnerabilities and leveraging years of specialization. Additionally, they have also demonstrated strong capabilities for exploiting weaknesses associated with smart contracts, solidifying their position as a key threat in this domain.

# Crypto-focused attacks

## A GROWING AND TARGETED INVOLVEMENT

The Lazarus Group was responsible for **$1,903,600,000** stolen in total across the web3 ecosystem from 2021 to 2023. In Q3 2023 alone, the group was responsible for $208,600,000 stolen, representing 30% of the total crypto losses in Q3. It was allegedly behind the high-profile attacks on CoinEx, Alphapo, Stake, and CoinsPaid. The biggest attack recorded to date was the one targeting Ronin Network, which resulted in a $625,000,000 loss.



# DeFi vs. CeFi Analysis

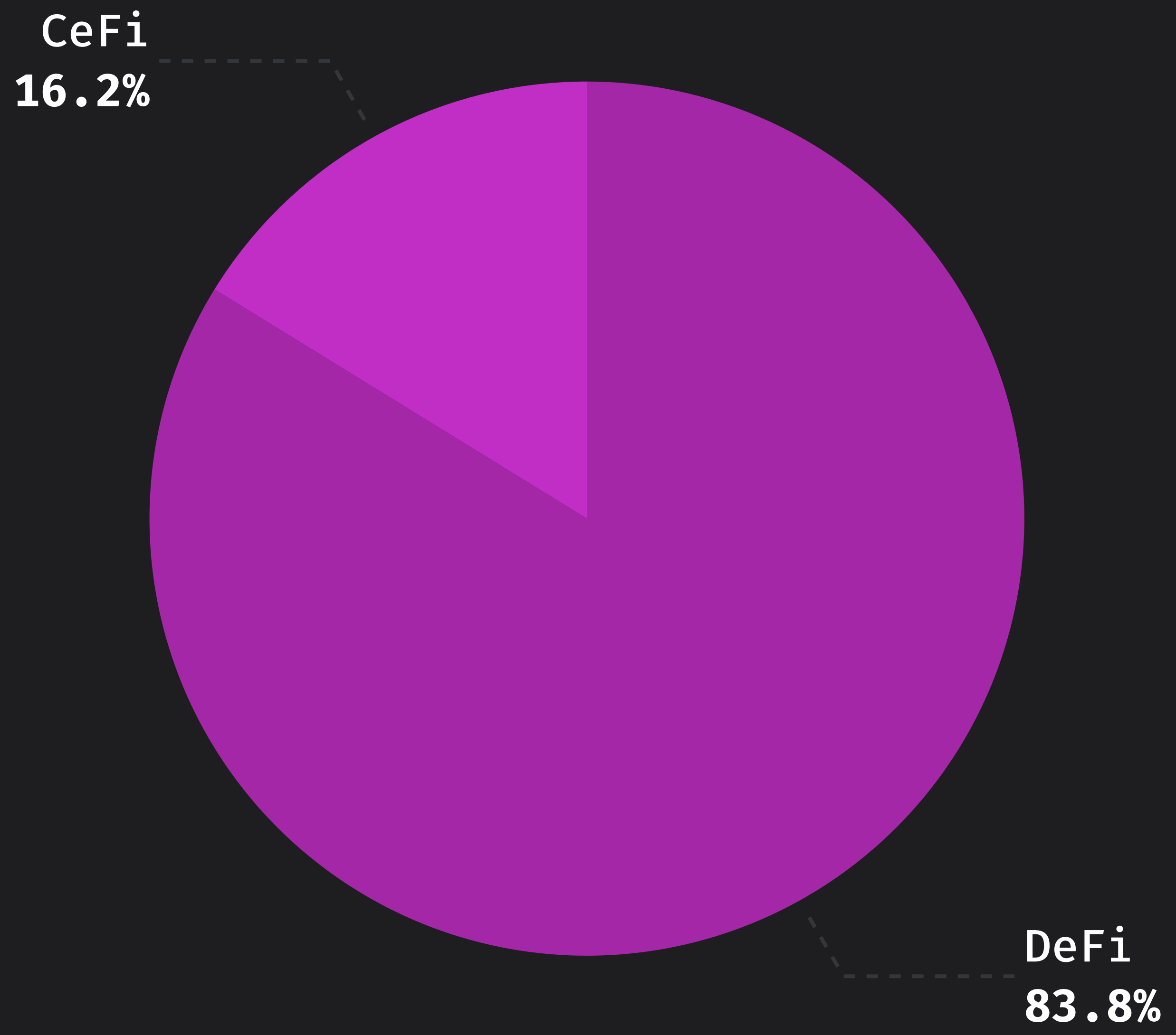
Between 2021 and 2023, DeFi represented 83.8% of the total attacks carried by the Lazarus Group, while CeFi represented 16.2%. These numbers are largely driven by the attacks on DeFi projects such as Ronin Network and Poly Network.

## OVERVIEW

- **DeFi**
  Lazarus Group attacks have resulted in a total loss of **$1,595,000,000** in 5 incidents within the DeFi sector.
- **CeFi**
  CeFi has suffered **$308,600,000** in total losses across 5 incidents.

## 2023: GROWING FOCUS IN CEFI

The shift towards targeting centralized services has become increasingly evident. Throughout 2023, **all reported Lazarus Group incidents unfolded within CeFi**, solidifying its status as the primary target for successful exploits carried out by Lazarus. The cases involve Atomic Wallet, CoinEx, Alphapo, Stake, and CoinsPaid, which collectively lost a staggering total of $308.6 million between June and September 2023.



# Laundering attempts

The Lazarus Group often employs sophisticated money laundering schemes to obscure the origins of its stolen funds, making it challenging for investigators to trace the money.

Initially, the stolen money might be sent to intermediary wallets, effectively disconnecting it from its source. Then, it is mixed in batches using mixing services. To further complicate the tracing process, hacker groups might also swap the chains, creating an additional layer of complexity. Then it is mixed in batches again, adding another level to the laundering operation.

These actions demonstrate Lazarus' expertise in utilizing various cryptocurrency mixing services and meticulous laundering operations.

Furthermore, groups located in hard-to-reach jurisdictions like Iran, Russia, and North Korea, have unique methods of cashing out cryptocurrencies into fiat currencies. For example, North Korean-backed organizations such as Lazarus are linked to the government and can rely on state-level connections to cash out into fiat through Chinese exchanges.

## IN FOCUS

### ATOMIC WALLET

A few days after the exploit, the hackers funneled the stolen crypto to Sinbad.io, a crypto mixer used by the Lazarus Group to launder crypto assets.

As the attack began to be tracked, Lazarus switched to the Russia-based Garantex exchange to continue laundering the stolen assets.

### COINSPAID

Hackers leveraged swap services, such as SunSwap, SwftSwap, and SimpleSwap, as well as Sinbad.io, to launder the funds without any KYC (costumer verification) or AML procedures in place, which are normally used to control money laundering, fraud, and financial crime.

Most of the stolen funds were sent in the form of USDT to the SwftSwap cryptocurrency service on the Avalanche-C blockchain. A small portion of the stolen funds was sent to the Yobit exchange.

# Private key handling

Recent incidents involving CoinsPaid, Alphapo, Stake.com, and CoinEx, for example, illustrate a common thread: Lazarus attackers breached the projects' hot wallets by compromising their private keys.

In light of this recent surge in attacks, it's crucial to underscore the importance of securing private keys. One key lesson learned is the necessity of maintaining private keys offline whenever feasible.

## SECURITY APPROACH

- Storing private keys on internet-connected devices exposes them to potential vulnerabilities, as evidenced by various malware and phishing attacks perpetrated by the Lazarus Group.
- To enhance security, consider using hardware wallets. Physical devices and private keys stored offline are much less susceptible to remote attacks. Additionally, implementing multi-signature wallets adds an extra layer of protection. With multi-signature, multiple private keys are required to authorize a transaction, reducing the risk associated with a single point of failure.
- Regularly updating and patching software is crucial. Outdated software can have known vulnerabilities that attackers can exploit.

# Centralized exchanges

According to CoinsPaid's report, Lazarus hackers dedicated half a year to surveilling and analyzing the exchange in an attempt to breach its systems and exploit weaknesses.

Their primary objective was to trick a key employee into installing software that would grant remote access to a computer, enabling them to breach and access CoinsPaid's internal systems. Despite six months of unsuccessful attempts, the hackers eventually succeeded in attacking CoinsPaid infrastructure.

Centralized exchanges are often examined by state-backed groups such as the Lazarus Group. For security purposes, it is crucial to monitor network activities, use machine learning and threat detection systems to recognizing attack patterns, and train and educate the team.

## SECURITY APPROACH

- Use advanced threat detection systems that can identify and respond to sophisticated attacks.
- Implement continuous monitoring of network activities. Unusual patterns or access attempts can be indicative of attack attempts.
- Engage in regular security audits, both internally and through third-party firms, to identify vulnerabilities. This includes reviewing infrastructure, code, and employee practices.
- Implement network segmentation to restrict access within the internal network. This limits the lateral movement of attackers, making it more challenging for them to navigate through the system. Use end-to-end encryption for sensitive data, both in transit and at rest. This adds an additional layer of protection in case of a breach.
- Enforce the use of multi-factor authentication for all access points, especially for privileged accounts. This adds an extra layer of security even if credentials are compromised.
- Train employees on security best practices and raise awareness about potential threats like phishing attempts. Ensure that staff members are vigilant against social engineering tactics.

# Social engineering

The notorious attack on the Ronin Network was executed through a social engineering operation. Lazarus managed to convince a senior engineer from Axie Infinity to apply for a job at a fictitious company. The job offer, presented in a PDF document, served as a vehicle for spyware, enabling hackers to breach Ronin's systems.

Lazarus has a history of using fake job offers as a social engineering tactic, which they have mastered and often execute with meticulous detail and patience.

Web3 projects and users have persistently been targeted with such social engineering operations that can lead to direct access to systems and catastrophic losses. While the focus has been on securing smart contracts, the urgency to educate about other attack vectors has never been greater.

## SECURITY APPROACH

- Inform users and team members about phishing techniques and social engineering tactics that attackers often employ. Being cautious with emails, messages, and online communications, especially those requesting sensitive information, is essential.

> “
>
> In 2023, Lazarus exclusively targeted centralized finance (CeFi) projects. As we approach 2024, their escalating sophistication is concerning. Their proficiency in exploiting infrastructure vulnerabilities, smart contract weaknesses, as well as their meticulous social engineering operations, underscores their emergence as perhaps the most pressing threat to web3 today.

**Mitchell Amador**

Founder and CEO at Immunefi

# Immunefi

Immunefi is the leading blockchain cybersecurity platform protecting over $50 billion in user funds. Immunefi operates the biggest community of blockchain security researchers who review projects' blockchain and smart contract code, find and responsibly disclose vulnerabilities, and get paid for making crypto safer. With Immunefi, researchers are rewarded based on the severity of the vulnerability that they discover, creating incentives for as many experts as possible to examine project code for vulnerabilities.

## PIONEERING STANDARD

Immunefi has pioneered the scaling web3 vulnerability disclosure standard, meaning that rewards should be priced accordingly with the severity of an exploit and the volume of funds at risk, which resulted in the company building the largest community of security talent in the web3 space.

## TOTAL BOUNTIES PAID

Immunefi has paid out over **$85 million** in total vulnerability rewards, while saving over **$25 billion** in user funds.

## TOTAL BOUNTIES AVAILABLE

Immunefi offers over **$150 million** in available vulnerability rewards.

## SUPPORTED PROJECTS

Trusted by established, multi-billion dollar web3 projects like Chainlink, Wormhole, MakerDAO, TheGraph, Synthetix, and more, Immunefi now supports more than 300 projects across multiple crypto sectors.

## LARGEST VULNERABILITY REWARDS PAID IN THE HISTORY OF SOFTWARE

Immunefi has facilitated the largest payments in the history of software:

- **$10 million** for a vulnerability discovered in Wormhole, a generic cross-chain messaging protocol.
- **$6 million** for a vulnerability discovered in Aurora, a bridge, and a scaling solution for Ethereum.
- **$2.2 million** for a vulnerability discovered in Polygon, a decentralized Ethereum scaling platform that enables developers to build scalable, user-friendly dApps.

**Disclaimer**:

- Immunefi uses publicly available data and news reports in order to access and collect attacks allegedly carried out by the Lazarus Group.

**Notes:**

- Poly Network: Hackers linked with Lazarus Group are suspected to be responsible for the attack.
- Qubit: Hackers linked with Lazarus Group are suspected to be responsible for the attack.
- Ronin Network: An FBI investigation revealed that Lazarus Group is allegedly behind the attack.
- Harmony: An analysis of the data suggests that the Lazarus Group is behind the attack.
- Nomad: The Lazarus Group is suspected to be behind the attack on Nomad bridge. The U.S. Treasury has openly accused North Korea of being involved in the theft of about $7.8 million.
- Atomic Wallet: The Lazarus group is suspected to be responsible for the attack that hit more than 5,500 digital wallets.
- CoinsPaid: According to a report from CoinsPaid, the Lazarus Group is suspected to be behind the attack.
- Alphapo: The Lazarus Group is suspected to be responsible for the attack.
- Stake.com: An FBI investigation revealed that Lazarus Group is allegedly behind the attack.
- CoinEx: The Lazarus Group is suspected to be responsible for the attack.

**More**:

- If you're a developer thinking about a bug-hunting career in web3, we got you. Check out our **Web3 Security Library**, and start taking home some of the more than $150M in rewards available on Immunefi — the leading bug bounty platform for web3.

For more information, please visit **https://immunefi.com/**