

# OpenVoiceNews India

Transparent. Unbiased. Yours.

## 2020 \$3.5 Billion Bitcoin Mining Pool Hack Uncovered by Arkham Intelligence

August 3, 2025

– Categories: *Crypto*



Download IPFS

A massive Bitcoin (BTC) theft from 2020 has been brought to light, revealing what is now considered the largest cryptocurrency hack in history. Blockchain analytics firm Arkham Intelligence reported that Chinese mining pool LuBian lost 127,426 BTC, valued at approximately \$3.5 billion at the time, after a security breach on December 28, 2020.

According to Arkham, LuBian ranked as the sixth-largest Bitcoin mining pool at the time of the incident. The attackers managed to seize roughly 90% of the pool's Bitcoin holdings before LuBian moved the remaining 11,886 BTC to recovery wallets. Neither the mining pool nor the hackers publicly disclosed the attack in 2020.

The stolen Bitcoin, now valued at approximately \$14.5 billion based on current market prices, was traced to multiple wallet addresses associated with the perpetrator. Arkham noted that LuBian embedded an "OP\_RETURN" message, an instruction allowing arbitrary data to be stored on the blockchain, into 1,516 transactions directed at the hacker's wallets, at a cost of about 1.4 BTC.

Arkham's investigation suggests the vulnerability may have stemmed from LuBian's method of generating private keys. The firm stated that the pool appeared to use an algorithm susceptible to brute-force attacks, enabling hackers to gain unauthorized access to its funds.

This revelation surpasses the scale of the February 2025 ByBit exchange hack, previously considered the largest in history. The ByBit breach, which resulted in the theft of \$1.5 billion worth of cryptocurrency, was attributed to a compromised developer machine linked to SafeWallet, a cryptocurrency wallet provider. A joint report by SafeWallet and cybersecurity company Mandiant indicated that malware was installed on the developer's system, allowing the attackers to exploit active Amazon Web Services (AWS) tokens.

The LuBian case underscores the importance of robust security practices in the cryptocurrency sector, particularly for managing private keys. Arkham emphasized the necessity of using strong random number generators and implementing proactive safeguards to prevent similar incidents.

With the value of the stolen Bitcoin having increased significantly since 2020, the breach serves as a stark reminder of the long-term consequences of cybersecurity failures in the digital asset space. The incident also highlights how some of the most significant attacks in the industry can remain hidden for years before coming to light.