A hacker stole $625 million from the blockchain behind NFT game Axie Infinity

By Adi Robertson, Corin Faife

Published: 2022-03-29 · Archived: 2026-04-29 07:15:39 UTC

Roughly $625 million worth of cryptocurrency has been stolen from Ronin, the blockchain underlying popular crypto game *Axie Infinity*. Ronin and *Axie Infinity* operator Sky Mavis revealed the breach on Tuesday and froze transactions on the Ronin bridge, which allows depositing and withdrawing funds from the company's blockchain.

Sky Mavis says it's working with law enforcement to recover 173,600 Ethereum (currently worth around $600 million) and 25.5 million USDC (a cryptocurrency pegged to the US dollar) from the culprit, who withdrew it from the network on March 23rd. The attack focused on the bridge to Sky Mavis' Ronin blockchain, an intermediary between *Axie Infinity* and other cryptocurrency blockchains like Ethereum. Users could deposit Ethereum or USDC to Ronin, then purchase non-fungible token items or in-game currency, or they could sell their in-game assets and withdraw the money.

According to Sky Mavis, an attacker used hacked private security keys to compromise the network nodes that validate transfers to and from the Ronin blockchain. That let the attacker quietly withdraw large quantities of Ethereum and USDC. The transfer was discovered today — nearly a week later — when another user attempted to withdraw 5,000 Ethereum through the bridge.

"As we've witnessed, Ronin is not immune to exploitation"

Sky Mavis says the "axie" NFT tokens players must buy to access *Axie Infinity* haven't been compromised, nor have the SLP and AXS in-game cryptocurrencies used in battling and breeding the pokémon-like cartoon axolotls. (Disclosure: Adi purchased three axies for a total of $105 last month in order to report on the game; axies currently sell starting at around $25 apiece.) But the freezing of withdrawals and deposits effectively locks out many new players, and the hack leaves the fate of other user funds on the Ronin blockchain in question. Sky Mavis says it's "working with law enforcement officials, forensic cryptographers, and our investors to make sure there is no loss of user funds," calling that its "top priority."

Validator nodes are a feature of proof-of-stake blockchains like Ronin, which are less energy intensive than proof-of-work systems like Bitcoin and Ethereum. The nodes review new transactions to confirm that their inputs and outputs match and that authorization signatures are valid, rejecting any transactions that don't conform. Using a smaller number of nodes is faster and more efficient — but as the hack shows, it can create security risks if a majority of the nodes are compromised. It's a potential vulnerability for blockchains that are touted as both cheaper and more environmentally friendly than Ethereum.

Validator nodes are a key feature of less energy-intensive blockchains

According to Sky Mavis, the Ronin attack was possible partly because of a shortcut the company had taken to relieve an “immense user load” on its network in November of last year — months after the game exploded in popularity in the Philippines and other countries where players relied on it as a full-time job. The system was discontinued in December, but the permissions that allowed it were never revoked. In addition to compromising four of Sky Mavis’ own nodes, the attacker exploited them to get access to one managed by the community-owned Axie DAO. After compromising five of the nine validator nodes, the attacker could effectively override any transaction security and withdraw whatever funds they liked.

Sky Mavis says it will increase the required number of nodes to eight for transactions, and it will reopen the Ronin bridge “at a later date” once it’s certain no more funds can be drained. For now, the Ronin breach appears to be the largest hack to date of “decentralized finance” networks, coming on the heels of a $322 million theft from the bridge protocol Wormhole last month.

“As we’ve witnessed, Ronin is not immune to exploitation and this attack has reinforced the importance of prioritizing security, remaining vigilant, and mitigating all threats,” the company said in its announcement. “We know trust needs to be earned and are using every resource at our disposal to deploy the most sophisticated security measures and processes to prevent future attacks.”