Re: SEC, SR-NASDAQ-2023-016

From: Jayson Hobby, Compound Companies and Ethereum Enterprise Alliance

Date: 18/11/23

SEC:

It is important that this proposal be rejected on grounds relating to both hacking, and more importantly reverse-hacking.

Spot Bitcoin and Ether publicly listed ETFs have well-known hacking vulnerabilities. Losses can occur on any decentralized or centralized platform whether spot crypto is in transit or dormant. Because of the nature of the assets, their trading and systems (poor or no compliance, poor controls, and little to no regulatory oversight), there's generally little or no remedy for a hack or loss.

Here the sponsor does nothing to address losses in custody or otherwise, merely disclosing that the average ETF investors will wear this risk - there's no way the average retail investor has any ability to evaluate, hedge or prepare for this risk transfer.

An even bigger risk seemingly missed by everyone is crypto provenance. That is, if the Trust owns crypto, how are we sure that those coins or tokens are not the product of an alleged hack from months or years earlier, only for the crypto to be "reverse hacked" out of the Trust's assets on the instructions of a U.S. or foreign court order. This reverse theft has happened a number of times, but is kept silent by crypto operators and their counsel.

One of the largest hacks was conducted by a combination of Oasis and Summerfi and based on a yet to be released UK court order.

Sincerely,

JH

BRIAN QUARMBY FEB 25, 2023

Jump Crypto and Oasis.app ‘counter exploits’ Wormhole hacker for $225M

The asset retrieval came after the High Court of England and Wales ordered Oasis.app to work with Jump Crypto to recover the stolen funds.

19716 60 2:40

Collect article Own this piece of history as an NFT

Web3 infrastructure firm Jump Crypto and decentralized finance (DeFi) platform Oasis.app have conducted a “counter exploit” on the Wormhole protocol hacker, with the duo clawing back $225 million of digital assets and transferring them to a safe wallet.

The Wormhole attack occurred in February 2022, with roughly $321 million worth of wrapped ETH (wETH) exploited via a vulnerability in the protocol's token bridge.

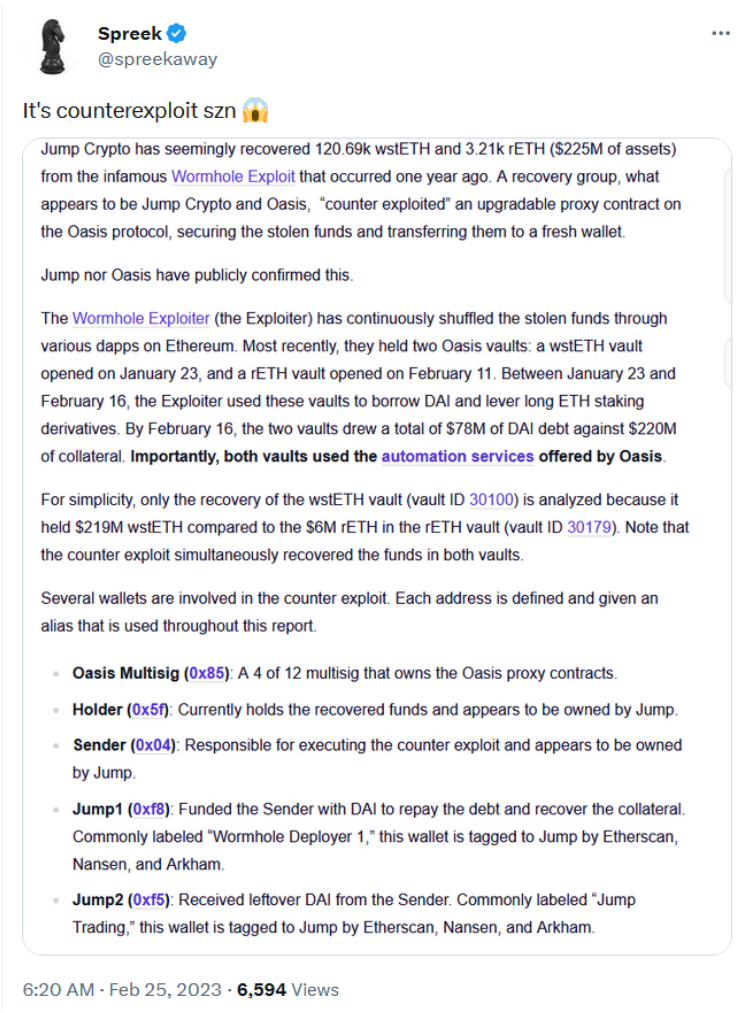
The hacker has since moved the stolen funds through various Ethereum-based decentralized applications (DApps), such as Oasis, which recently opened up wrapped stETH (wstETH) and Rocket Pool ETH (RETH) vaults.

In a Feb. 24 blog post, the Oasis.app team confirmed that a counter exploit had taken place, outlining that it had "received an order from the High Court of England and Wales" to retrieve certain assets related to the "address associated with the Wormhole Exploit."

The team stated that the retrieval was initiated via "the Oasis Multisig and a court-authorized third party," which was identified as Jump Crypto in a preceding report from Blockworks Research.

around $78 million debt in MakerDAO's Dai DAI ▼ $1.00 stablecoin, which was retrieved.

"We can also confirm the assets were immediately passed onto a wallet controlled by the authorized third party, as required by the court order. We retain no control or access to these assets," the blog post reads.



@spreekaway tweet on the counter exploit. Source: Twitter

Referencing the negative implications of Oasis being able to retrieve crypto assets from its user vaults, the team emphasized that it was “only possible due to a previously unknown vulnerability in the design of the admin multisig access.”

Related: DeFi security: How trustless bridges can help protect users

The post stated that such a vulnerability was highlighted by white hat hackers earlier this month.

“We stress that this access was there with the sole intention to protect user assets in the event of any potential attack, and would have allowed us to move quickly to patch any vulnerability disclosed to us. It should be noted that at no