Qubit Finance’s Heist Underscores Why an Able MSP is Pertinent

In recent times, roping in a Managed Services Provider (MSP) or third-party security contractor has become the new normal as managing the affairs single-handedly has become an arduous task. This demand has led to MSPs’ cropping up almost everywhere, and this trend shall only increase as the world is increasingly integrating with cloud technologies.

However, some companies opted for a different approach, such as smart contracts, which has only come back to bite them and Qubit Finance’s heist reflects the same.

Built on Binance Smart Chain, threat actors have targeted **Qubit Finance** and have committed a theft of USD 80 million. This is 2022’s biggest cryptocurrency yet. A total of 2,06,809 Binance Coins were robbed from The QBridge protocol of Qubit. Qubit Finance acknowledged the heist with a tweet. “The team is currently working with security and network partners on next steps. We will share further updates when available," stated the tweet.

The Incident

This incident and all such heists that marred 2021 impress the viewpoint of how pertinent it is to establish robust protocols that are immune to thefts. Despite the best intentions, a gaping hole or ill-suited protocols allow threat actors to implement their nefarious strategies.

PeckShield, the security firm that audited Qubit's smart contracts, echoed similar sentiments. It concluded that the QBridge was breached, allowing the threat actors to get a "huge amount of xETH collateral". This collateral was then exploited to swipe all of the Binance Coins housed in QBridge.

Qubit Finance employed smart contracts to ensure that their customers have the trading, lending, and borrowing facilities. This choice has led the DeFi firm to rely on these contracts rather than third-party contractors. Users are required to credit the **QBridge** with their cryptocurrency holdings. The protocol allows the users to be footloose by collateralizing their assets on other domains without offloading their assets on other networks.

Due to this offbeat option of smart contracts and QBridge, the threat actors exploited a deposit option in the protocol to illegally create 77,162 qXETH, an asset on Qubit which represents Ether. The protocol assumed that the threat actors made a deposit which they never did. The hackers repeated these ‘deposits’ and converted all of the non-existent deposits to Binance coins.

Useful Link: **GitOps. What’s it all about?**

Aftermath

The **DeFi company** stated that the impacted assets were being monitored. It elaborated that they reached out to the threat actor to tender a “maximum bounty offer,” which was calculated with their program. This has adversely impacted Qubit’s image as their stock fell drastically after this incident. This is all the more the reason as to why one should consider roping in an MSP that can fortify the assets and swat away threats as they arise.

With due diligence, Fortune 500 and emerging enterprises have roped in **Veritis** and secured their assets. We have created cost-effective and robust future-proof solutions which have helped our clients pursue their business goals better and faster.

So, get in touch with us and walk away with a solution that protects your company better.

Services