POLY NETWORK HACK: THE BIGGEST DeFi THEFT IN HISTORY

Pratham Arora, *Risk Intelligence Consultant*

EXECUTIVE SUMMARY

- On 10 Aug 2021, hackers stole more than $600 Million in cryptocurrency from Decentralized Finance (DeFi) firm Poly Network.
- Dubbed as the largest cryptocurrency theft ever, the hacker stole money in the form of various cryptocurrencies.
- The money was rendered unusable soon as a part of it was blocked and other parts could not be laundered.
- The hacker(s), being called Mr. White Hat, named after benign hackers who find flaws in coded systems, started returning the money within 48 hours, having returned most of it by 12 Aug 2021.
- As of 24 Aug 2021, the hacker has returned all of the money they stole.
- The hacker was also awarded a $500,000 bug bounty and was offered a job by Poly Network.

POLY NETWORK

PolyNetwork

POLY NETWORK:

- A relatively lesser known entity in the crypto world, Poly Network is a DeFi platform that focuses on peer-to-peer transactions, especially across different blockchains.
- DeFi platforms allow people to lend or borrow funds from others, speculate on price movements on a range of assets using derivatives, trade cryptocurrencies, insure against risks, and earn interest in savings-like accounts
- Poly Network was founded by Chinese entrepreneur Da Hongfei, who is currently chief executive of Neo, a blockchain platform. It was launched as a collaboration between Neo, Switcheo, and Ontology.

WHAT WAS STOLEN, AND WHERE DID IT GO?

The hacker stole cryptocurrency worth $610 Million in 12 different types of currencies, including Ether, Binance, and Polygon.

STOLEN ASSET	AMOUNT STOLEN
Ethereum	$273 million
Binance Smart Chain	$253 million
Polygon	$85 million

The hacker first attempted to transfer some assets into liquidity pool Curve.fi, but the transfer was rejected. About $100 Million was moved to liquidity pool Ellipsis Finance.
Later, around 11 Aug 2021, the hackers started moving the money back Poly Network. By 12 Aug 2021, only $31 Million in tokens, frozen by the platform Tether, were left.

HOW DID THE HACK TAKE PLACE?

The three blockchain Poly Network uses, Binance, Ethereum, and Polygon, all make use of something known as a smart contract. In a nutshell, a smart contract tells a computer when to release assets to the counterparties.

For efficiency in transferring tokens between blockchains, one of the smart contracts used maintained a large amount of liquidity. Furthermore, it was coded such that a brute-force attack, that is, an attack which tries a lot of different combinations for a key using trial and error, could exploit the code.

Said brute force attack basically transferred the control of the smart contract to the hacker, who could then transfer the currencies to 3 different wallets.

A person claiming to be the hacker later said they just wanted to expose the vulnerability before someone could make use of it.

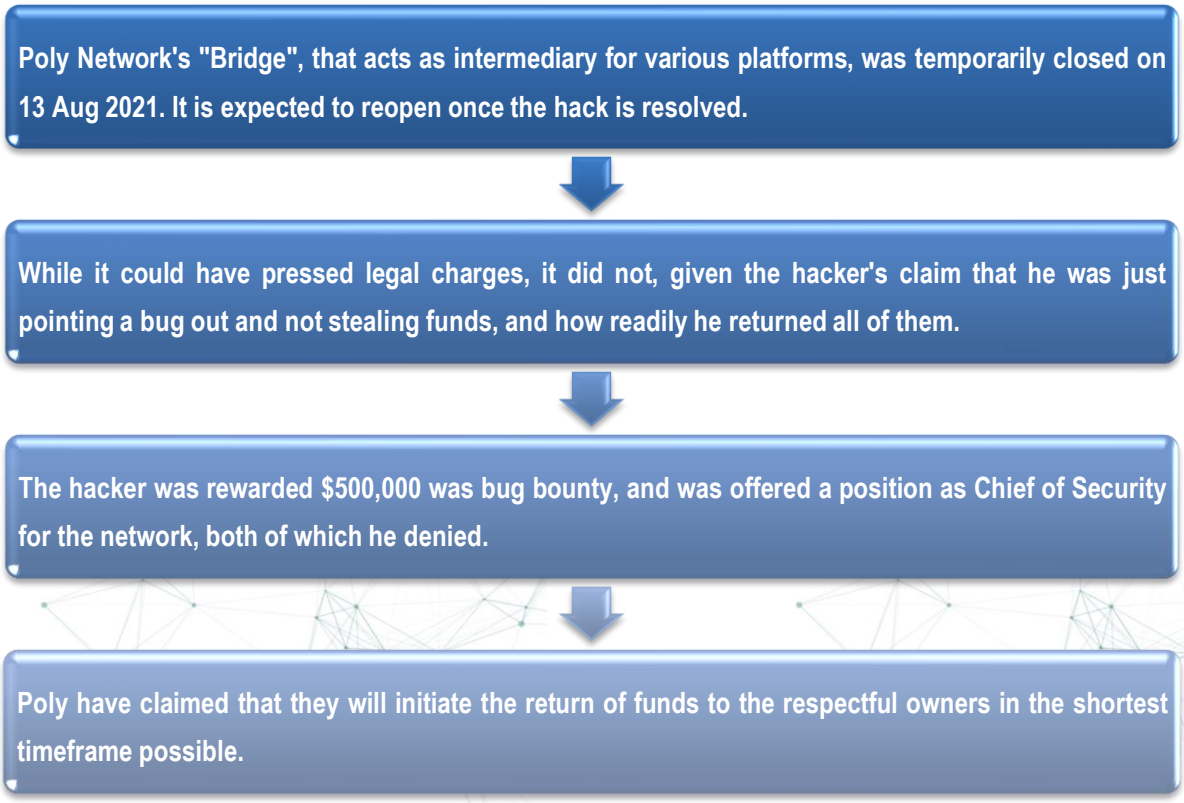
THE HACKER(S)

The hacker is unidentified as of yet. Cryptosecurity firm SlowMist claims to have the attacker's mailbox, internet protocol address, and device fingerprints, but no ID yet. The firm claims the attack was "likely to be a long-planned, organized and prepared."

Despite the purported hacker posing as a so-called "white hat", an ethical hacker who had "always" planned to give the money back some crypto experts are skeptical. Gurvais Grigg, chief technology officer at Chainalysis and former FBI veteran, said on Wednesday that it was unlikely that white hat hackers would steal such a large sum. According to him, the funds were likely returned because of difficulties in laundering it.

The hacker himself, however, returned more than he stole, giving away some of the bug bounty of $500,000 he earned as compensation to the people affected.

POLY NETWORK'S REACTION



Given this and other attacks on DeFi systems, it seems that this new, evolving technology is vulnerable and has to evolve quick to be safe. DeFi-related hacks at $361 million account for 76% of crypto-hacks so far this year. This is against $129 million or 25% of the total crypto hacks for all of the year 2020.

OTHER ATTACKS FROM 2021:

Month	Entity	Loss
July 2021	THORChain	$13 million
July 2021	ChainSwap	$8.8 million
May 2021	Rari Capital	$10 million
May 2021	PancakeBunny	$45 million

ASSESSMENT

This hack was centered around a system that tries to interoperate various different blockchains, and not one specific blockchain. This highlights the vulnerability of the system which liaisons between different cryptos. However, prominent cryptocurrencies are safe, owing to their built-in security architecture, their decentralized nature and continuous bug fixes by the community.

Additionally, while the currencies were successfully transferred, they were rendered unusable since they could not be laundered and a part of them was blocked. That being said, caution must be observed with regards to new technology related to cryptocurrency, a market that is evolving with a lot of money and hype around it. An end user, with only basic understanding of technology, may not be able to understand its vulnerabilities.

This time, it was a white-hat hacker, however someone with motives to genuinely steal the money may also exploit these bugs. Thus, it is important to cater to investments regarding internal security of cryptocurrencies market, and not confine only to the innovation and fast-evolving technology aimed at enhancing the market.

ABOUT THE AUTHOR

Pratham Arora: Is a Risk Intelligence Consultant at WoRisGo. He is currently an undergraduate at Ashoka University, studying Political Science, International Relations, and Philosophy. His primary areas of interest include Diplomacy, International Relations theory, and Conflict Analysis.