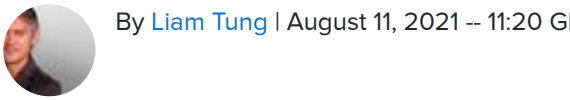
MUST READ: Need developers? Solving the tech skills shortage means looking beyond hiring

Hackers take $600m in 'biggest' cryptocurrency theft

Updated: Poly Network has asked for 'hacked assets' to be returned by attackers - and it has apparently received millions back already.



By Liam Tung | August 11, 2021 -- 11:20 GMT (04:20 PDT) | Topic: Security

A hacker has apparently exploited a vulnerability to steal $600 million from a blockchain finance platform in what could be one of largest cryptocurrency thefts to date.

The makers of Poly Network, a "DeFi" or decentralized finance platform that works across blockchains, said on Tuesday that an attacker stole about $600 million in cryptocurrencies.

The team behind Poly Network appealed to the hackers (https://twitter.com/PolyNetwork2/status/1425123153009803267) to "return the hacked assets".

"The amount of money you hacked is the biggest one in defi history. Law enforcement in any country will regard this as a major economic crime and you will be pursed. It is very unwise for you to do any further transactions. The money stole are from tens of thousands of crypto community members, hence the people. You should talk to us to work out a solution," the Poly Network team said.

SEE: This new phishing attack is 'sneakier than usual', Microsoft warns (https://www.zdnet.com/article/microsoft-watch-out-for-this-sneakier-than-usual-phishing-attack/)

Poly Network works across blockchains for Bitcoin, Ethereum, Neo, Ontology, Elrond, Ziliqa, Binance Smart Chain, Switcheo, and Huobi ECO Chain.

Poly Network listed three addresses the assets were transferred to.

(https://adclick.g.doubleclick.net/pcs/click%253Fxai%253DAKAOjsshtTlFd_VODQw7x0yR37eqcSipC1VcUAEWJhqFerKxAZ5
bhGaYVlkGGp0N9cD1tR6e50LUw40McGGeyOVAAkN2oW3_qgSATWv18A4AyRZZ4ppgRXXV_ZocX66h4UnTmZ0OO_35Z
OYxcnCkWFE_60ujPYN9jpbRniMlJ7jskamVHWo29YCj5zA6NeZ5JjA%2526sig%253DCg0ArKJSzEAqKP4RoadFEAE%2526
edition=en&ursuid=&devicetype=desktop&pagetype=&assettitle=&assettype=&topicguid=&viewguid=a05b8207-b171-4e9a-
939e-683411712722&docid=6d38933c-24d8-4e26-9722-1bd0cf6b0aa1&promo=1065&ftag_cd=TRE-00-
10aaa4f&spotname=dfp-in-article&destUrl=https%253A%252F%252Fwww.techrepublic.com%252Farticle%252Fthe-best-
luggage-for-business-trips-as-offices-reopen-and-travel-picks-up%252F%253Fpromo%253D1065%2526cval%253Ddfp-in-

"We call on miners of affected blockchain and crypto exchanges to blacklist tokens coming from the above addresses," the team pleaded.

And it appears that at least a small amount of the funds have been returned. Poly Network posted on Twitter "you are moving things to the right direction" and said that it had received more than $1m back (https://twitter.com/PolyNetwork2/status/1425395278341820420).

A little later it posted again saying (https://twitter.com/PolyNetwork2/status/1425423585665974276): "So far, we have received a total value of $4,772,297.675 assets returned by the hacker. ETH address: $2,654,946.051 BSC address: $1,107,870.815 Polygon address: $1,009,480.809."

According to Poly Network (https://twitter.com/PolyNetwork2/status/1425130017546149891), "the hacker exploited a vulnerability between contract calls, exploit was not caused by the single keeper as rumored."

Per Wall Street Journal's MarketWatch (https://www.marketwatch.com/story/poly-network-pleads-for-hackers-to-return-assets-after-611-million-crypto-heist-11628650932), the CTO of stablecoin company Tether, Paolo Ardoino, said the company froze $33 million of its tokens lost in the Poly Network attack.

The hackers stole about $267m of Ether, $252m of Binance coins, and $85 million in USDC tokens.

SEE: Attacks on critical infrastructure are dangerous. Soon they could turn deadly, warn analysts (https://www.zdnet.com/article/attacks-on-critical-infrastructure-are-dangerous-soon-they-could-turn-deadly-warns-analyst/)

Changpeng Zhao "CZ", chief of the giant Binance crypto-exchange, said on Twitter (https://twitter.com/cz_binance/status/1425091869709570060) that it was aware of the Poly Network attack and noted that there was not much the company could do about it.

"While no one controls BSC (or ETH), we are coordinating with all our security partners to proactively help. There are no guarantees. We will do as much as we can," he wrote.

SECURITY

Kaseya ransomware attack: What you need to know (https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/)

Surfshark VPN review: It's cheap, but is it good? (https://www.zdnet.com/article/surfshark-vpn-review/)

The best browsers for privacy (https://www.zdnet.com/article/best-browser-for-privacy/)

Cyber security 101: Protect your privacy (https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

The best antivirus software and apps (https://www.zdnet.com/article/best-antivirus/)

The best VPNs for business and home use (https://www.zdnet.com/article/best-vpn/)

The best security keys for 2FA (https://www.zdnet.com/article/best-security-key/)

How victims who pay the ransom encourage more attacks (ZDNet YouTube) (https://www.youtube.com/watch?v=jGqHliuqWmc)

RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

By Liam Tung | August 11, 2021 -- 11:20 GMT (04:20 PDT) | Topic: Security

SHOW COMMENTS