Che cosa sappiamo del più grande furto di criptovalute di sempre



Più di 600 milioni di dollari sono stati sottratti alla piattaforma di finanza decentralizzata PolyNetwork, dopo un attacco informatico che è già entrato nella storia come uno dei più grandi furti di criptovalute di sempre. I gestori della piattaforma hanno rivelato l'attacco su Twitter, pubblicando poi una lettera in cui hanno chiesto ai criminali di restituire i beni violati.

Che cos'è PolyNetwork

PolyNetwork è una sistema di finanza decentralizzata (DeFi) che consente lo scambio di gettoni virtuali (token) tra

diverse piattaforme di blockchain, cioè i registri virtuali su cui si basa il funzionamento di diverse criptovalute. Ogni moneta digitale ha la propria blockchain, il proprio registro, su cui tiene traccia delle transazioni e dei beni, **il servizio offerto da PolyNetwork è di collegare tra loro le diverse blockchian**. Con il termine DeFi, inoltre, si indicano tutte le applicazioni finanziarie che cercano di operare senza intermediari, come i le borse e gli agenti di borsa.

> *Important Notice:*
> *We are sorry to announce that #PolyNetwork was attacked on @BinanceChain @ethereum and @0xPolygon Assets had been transferred to hacker's following addresses:*
> *ETH: 0xC8a65Fadf0e0dDAf421F28FEAb69Bf6E2E589963*
> *BSC: 0x0D6e286A7cfD25E0c01fEe9756765D8033B32C71*
>
> *— Poly Network (@PolyNetwork2) August 10, 2021*

Chi ha compiuto l'attacco

Nella lettera pubblicata da PolyNetwork, l'azienda si rivolge a un generico *"caro hacker"*. Tuttavia, **il termine hacker non ha una connotazione negativa**, ma indica chiunque è in grado di esplorare le potenzialità offerte da un sistema informativo e di metterne alla prova le sue capacità. Un hacker è quindi chi è in grado di comporre insieme diversi programmi, superando le procedure standard usate nella scrittura dei software e non ha nulla a che fare con la criminalità. **Chi usa queste competenze con intenti malevoli viene indicato con il nome di *cracker***, dal verbo inglese *to crack*, che significa spezzare, rompere, crepare.

> *1)The cross-chain interoperability protocol @PolyNetwork2 was attacked, and a total of more than 610 million US dollars were transferred to 3 addresses. The impact caused the transfer of large assets of the O3 Swap cross-chain pool.*

— *SlowMist (@SlowMist_Team) August 10, 2021*

Secondo quanto rivelato su Twitter da SlowMist, società di sicurezza informatica cinese, i *cracker* sarebbero riusciti a trasferire 610 milioni di dollari verso 3 diversi indirizzi collegati a 3 diverse criptovalute. Partendo da questi indirizzi, **i tecnici di SlowMist sarebbero stati già in grado di rintracciare l'indirizzo Ip degli attaccanti**, così come il loro indirizzo email e le loro impronte digitali. La società ha anche detto che queste informazioni sono state ottenute grazie alla collaborazione con Hoo, un'altra piattaforma di scambio di criptovalute cinese. SlowMist ha poi offerto a PolyNetwork di condividere con loro le informazioni ottenute.

La lettera di PolyNetwork

Poche ore dopo l'annuncio di SlowMist, l'account Twitter di PolyNetwork ha condiviso un'immagine con una lettera indirizzata ai cracker, **nella quale ha chiesto loro di essere contattata e di restituire tutti i fondi rubati**. Letteralmente, l'ultima riga recita *"dovreste parlare con noi per trovare una soluzione"*, dopo aver ricordato agli attaccanti che *"saranno ricercati dalle forze dell'ordine di tutti i paesi"*. Questo approccio può quindi suggerire due cose, o un'estrema disperazione oppure che la compagnia sia veramente in possesso di informazioni dettagliate rispetto all'origine dell'attacco.

pic.twitter.com/Yzw4oDenjC

— *Poly Network (@PolyNetwork2) August 10, 2021*