KRYPTO NEWS
PART OF THE GLOBAL WOM NEWS NETWORK
26. Juli 2022

Die neun größten Krypto-Hacks im Jahr 2022

Einzelne Zeilen schlecht durchdachten Codes verschafften Hackern Zugriff auf Kryptoassets im Wert von Hunderten Millionen Dollar Die meisten gehackten Unternehmen setzen ihren Betrieb fort, nachdem sie sich Audits unterzogen oder ihre Sicherheit verbessert haben Hacker nutzten einen Softwarefehler in der Web3-Musikplattform Audius aus, um am Samstag mit 1,1 Millionen US-Dollar davonzukommen, aber die Gelder sind ein Tropfen auf den fast 2-Milliarden-Dollar-Eimer, der laut Hackern im ersten Halbjahr 2022 verloren gegangen ist Blockchain-Sicherheitsfirma Beosin. Der Fiat-Wert gehackter Vermögenswerte ist auf dem besten Weg, die 3,2 Milliarden US-Dollar zu übertreffen, die im Jahr 2021 verloren wurden. laut der Krypto-Sicherheitsfirma Chainalysis, selbst inmitten …

- Einzelne Zeilen schlecht durchdachten Codes verschafften Hackern Zugriff auf Kryptoassets im Wert von Hunderten Millionen Dollar
- Die meisten gehackten Unternehmen setzen ihren Betrieb fort, nachdem sie sich Audits unterzogen oder ihre Sicherheit verbessert haben

Hacker nutzten einen Softwarefehler in der Web3-Musikplattform Audius aus, um am Samstag mit 1,1 Millionen US-Dollar davonzukommen, aber die Gelder sind ein Tropfen auf den fast 2-Milliarden-Dollar-Eimer, der laut Hackern im ersten Halbjahr 2022 verloren gegangen ist Blockchain-Sicherheitsfirma Beosin.

Der Fiat-Wert gehackter Vermögenswerte ist auf dem besten Weg, die 3,2 Milliarden US-Dollar zu übertreffen, die im Jahr 2021 verloren wurden. laut der Krypto-Sicherheitsfirma Chainalysis, selbst inmitten eines drastischen Rückgangs der Kryptowährungsbewertungen. Blockworks hat einige der größten Krypto-Hacks des Jahres zusammengestellt, um zu sehen, was schief gelaufen ist und wie sich Protokolle nach dem Hacken geschlagen haben.

- Krypto.com17. Januar, 35 Millionen Dollar
    - Ende Januar gelang es einem Hacker, die Zwei-Faktor-Authentifizierung auf der Krypto-Börse Crypto.com zu deaktivieren und Bitcoin und Ether aus Kundenkonten zu extrahieren. CEO Kris Marszalek zunächst verweigerte Kundengelder gingen verloren bevor er den Hack Tage später anerkennt. Das Unternehmen

sagte, es stelle als Reaktion auf den Exploit auf ȣMulti-Faktor-Authentifizierungȣ um.

- Qubit QBridge-Hack, 27. Januar, 80 Millionen Dollar
    - Ein Hacker manipulierte einen Smart-Contract-Bug auf der QBridge des Binance-basierten Qubit Finance, um verpackte Ether-Token zu prägen, ohne Geld einzuzahlen. Das verlorene Vermögen zwang die Entwickler hinter Qubit das Personal des Protokolls zu kürzen und als dezentrale autonome Organisation (DAO) neu zu klassifizieren.
- Wurmloch, 2. Februar, 325 Millionen Dollar
    - Ein Hacker nutzte intelligente Verträge auf der Solana-zu-Ethereum-Brücke aus, um verpackten Ether zu prägen und auszuzahlen, ohne Sicherheiten zu hinterlegen. Jump Crypto, die Risikokapitalgesellschaft hinter Wormhole, füllte die gestohlenen Gelder wieder auf, um Solana-basierte Plattformen von dem Hack betroffen zu halten. Wormhole hat sein Brückenportal umbenannt und hält derzeit über 480 Millionen US-Dollar. laut Kryptodatenfirma DeFi Llama.
- IRA Financial Trust8. Februar, 37 Millionen US-Dollar
    - Die kryptofokussierte Alters- und Rentenplattform wurde gestohlen, als Hacker auf einen ȣHauptschlüsselȣ zugriffen, der alle Sicherheitsmaßnahmen für Kundenkonten umging. IRA Financial Trust hat seitdem verklagt Gemini, die Krypto-Börse, wo Kundengelder gespeichert wurden, wegen angeblicher Fahrlässigkeit, die zum Hack geführt hat.
- Kasse, 22. März, 52 Millionen Dollar
    - Eine Reihe gefälschter Konten nutzte einen ȣunendlichen Münzfehlerȣ, um wertlose Sicherheiten für Cashios Stablecoin CASH zu hinterlegen. Das coin¸s Stift ist auf Null gefallen und hat sich nicht erholt, nach Angaben von

CoinGecko.

- Axie Infinity Ronin-Brücke28. März, 625 Millionen US-Dollar
    - Der bisher größte Krypto-Hack, gemessen in Fiat-Dollar, erfolgte, nachdem Hacker die Kontrolle über einen Großteil der kryptografischen Schlüssel erlangt hatten, die die Cross-Chain-Bridge des Play-to-Earn-Spiels sichern. Vier der neun Schlüssel wurden gestohlen, als ein Axie-Entwickler auf ein gefälschtes Stellenangebots-PDF klickte. laut The Block. Die Ronin-Brücke wurde seitdem mit mehr Prüfern wiedereröffnet, obwohl das Spiel den Benutzern Blutungen bereitet.
- Bohnenstange, 17. April, 182 Millionen Dollar
    - Ein Hacker nutzte ein ȝFlash-Darlehenȝ, bei dem Gelder in derselben Transaktion geliehen und zurückgezahlt werden, um genügend Vermögenswerte anzuhäufen, um das Governance-Protokoll der Stablecoin zu kontrollieren. Der Hacker verabschiedete einen Vorschlag, Gelder an die Ukraine zu spenden, bevor er sich mit den Sicherheiten davonmachte. Die Entwickler pausierten das Protokoll, während sie sich Audits unterzogen und Spenden sammelten, aber planen, Einlagen wieder zu eröffnen Anfang August.
- Fei-Protokoll, 30. April, 80 Millionen Dollar
    - Ein ȝWiedereintrittsfehlerȝ im Code des Kreditprotokolls ermöglichte es einem Hacker, einen Kredit aufzunehmen und gleichzeitig die für den Kredit gestellten Sicherheiten abzuheben. Fei-Benutzer einen Vorschlag verabschiedet um Investoren gesund zu machen, indem ȝdas DAO die uneinbringlichen Schulden im Namen des Hackers zurückzahltȝ. Der Fei Stablecoin bleibt an seiner Dollarbindung, pro CoinGecko.
- Harmonie-Brücke23. Juni, 100 Millionen Dollar

- Die mit Nordkorea verbundene Lazarus-Gruppe griff auf zwei der fünf Sicherheitsschlüssel der Binance- und Ethereum-Brücke zu und genehmigte Transaktionen, bei denen Vermögenswerte von der Brücke abgezogen wurden. Harmonie jetzt erfordert vier von fünf Prüfschlüsseln einen Konsens über Transaktionen zu erzielen, und muss noch seinen Plan bekannt geben, Benutzer zu entschädigen.

Der Beitrag Die neun größten Krypto-Hacks im Jahr 2022 ist keine finanzielle Beratung.

Details