

Der andauernde Kampf gegen Kryptodiebe | FT-Tech

Sie können Untertitel (Bildunterschriften) im Videoplayer aktivieren Im März dieses Jahres führten Hacker einen der größten Kryptowährungsbetrübe aller Zeiten durch. Es reiht sich in eine wachsende Liste von Sicherheitsverletzungen bei Kryptowährungen ein, wie zum Beispiel der Diebstahl von mehr als 600 Millionen US-Dollar an Kryptowährungen aus dem Poly Network-Programm im vergangenen August. Im Jahr 2021 wurden Kryptowährungen im Wert von rund 3,2 Milliarden US-Dollar gestohlen, eine Steigerung von 516 Prozent gegenüber dem Vorjahr. Ein Faktor, der das antreibt Hacker, die das fünffache Wachstum des dezentralisierten Finanz- oder DeFi-Raums im letzten Jahr ausnutzen, wo Algorithmen alle Transaktionen abwickeln und es …

Sie können Untertitel (Bildunterschriften) im Videoplayer aktivieren

Im März dieses Jahres führten Hacker einen der größten Kryptowährungsbetrübe aller Zeiten durch. Es reiht sich in eine wachsende Liste von Sicherheitsverletzungen bei Kryptowährungen ein, wie zum Beispiel der Diebstahl von mehr als 600 Millionen US-Dollar an Kryptowährungen aus dem Poly Network-Programm im vergangenen August. Im Jahr 2021 wurden Kryptowährungen im Wert von rund 3,2 Milliarden US-Dollar gestohlen, eine Steigerung von 516 Prozent gegenüber dem Vorjahr. Ein Faktor, der das antreibt Hacker, die das fünffache Wachstum des dezentralisierten Finanz- oder DeFi-Raums im letzten Jahr ausnutzen, wo Algorithmen alle

Transaktionen abwickeln und es keine menschliche Interaktion zwischen den Parteien gibt.

Etwa 2,2 Milliarden Dollar an Geldern wurden aus DeFi-Projekten gestohlen, eine Steigerung von 1.330 Prozent gegenüber 2020. Für Inhaber digitaler Vermögenswerte bleibt eine sichere Speichertechnologie von entscheidender Bedeutung. Inhaber verwenden einen einzigartigen, privaten Schlüssel, ein langes Passwort, um auf ihre Krypto zuzugreifen. Die Schlüssel und damit Krypto können in Online- oder mobilen Wallets aufbewahrt werden, die einen schnellen Zugriff ermöglichen, aber die am wenigsten sichere Methode zur Aufbewahrung von Krypto bieten. Eine sicherere Alternative verwendet ein Gerät, das nicht mit dem Internet verbunden ist, bekannt als Cold Storage. Zu den Optionen gehören physische USB-Geräte, Offline-Computer oder ausgeklügelte Hardware-Wallets, kleine USB-ähnliche Geräte.

Aber auch andere spezialisierte Drittanbieterdienste schützen die Krypto-Assets der Kunden, indem sie beispielsweise private Schlüssel in Tresoren aufbewahren, die von menschlichen Wachen oder Systemen mit Gesichtserkennung und Fingerabdrücken geschützt werden. Betrug, Ransomware und Diebstahl sind im vergangenen Jahr in Dollar ausgedrückt um 79 Prozent gestiegen. Trotzdem stellten Transaktionen mit illegalen Adressen im Jahr 2021 mit nur 0,15 Prozent des gesamten Krypto-Handelsvolumens ein Allzeittief dar. Und Strafverfolgungsbehörden und Aufsichtsbehörden sind besser geworden, wenn es darum geht, Verbrechen im Zusammenhang mit Kryptowährungen zu bekämpfen.

Cyberkriminelle setzen jedoch zunehmend ihre eigenen Hightech-Tools und -Techniken ein, um der Entdeckung zu entgehen. Eine davon ist Chain-Hopping, das Springen zwischen verschiedenen Kryptowährungen, oft in schneller Folge. Eine andere beinhaltet die Verwendung von Tumblern oder Mixern, Diensten von Drittanbietern, die illegale Gelder mit sauberen Kryptos mischen, bevor sie sie neu verteilen. Rund 15 Prozent

aller Erlöse aus Straftaten flossen 2021 über Mixer. Mixer lassen sich aber zunehmend aussortieren. Und das Verschleiern großer Geldmengen durch Mixer kann für Kriminelle schwierig sein. Unterdessen gehen Aufsichtsbehörden und Strafverfolgungsbehörden zunehmend gegen illegale Transaktionen vor.

Im März forderte beispielsweise die britische National Crime Agency eine Regulierung dezentralisierter Krypto-Mischungen, während der Gesetzgeber der Europäischen Union strengere Rückverfolgbarkeitsregeln für den Transfer von Kryptowährungen unterstützte. Veränderung wird erwartet. Aber in einer Branche, in der die Teilnehmer daran gewöhnt sind, sich schnell zu bewegen, bleibt die Verantwortung bei den Regulierungsbehörden, Schritt zu halten.

Quelle: [Financial Times](#)

Details

Besuchen Sie uns auf: krypto-news.at