483 Crypto.com accounts compromised in $34 million hack

By
Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)

January 20, 2022 04:10 AM **0**

Crypto.com has confirmed that a multi-million dollar cyber attack led to the compromise of around 400 of its customer accounts. Although, the company's CEO stresses that customer funds are not at risk.

With regards to daily trading volume, Crypto.com is reportedly (https://archive.is/hsdqW) the world's third-largest cryptocurrency trading platform "on a mission to accelerate the world's transition to

cryptocurrency."

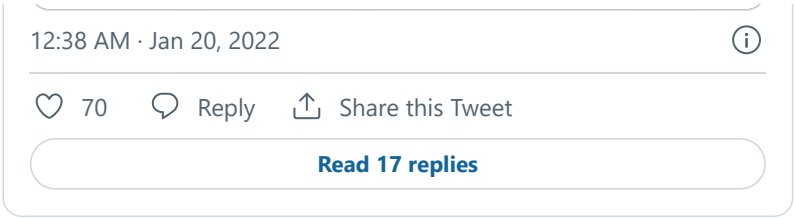
Crypto.com CEO: 400 customer accounts hit

In an interview with Bloomberg Live, Crypto.com's CEO Kris Marszalek acknowledged that around 400 customer accounts were compromised following a recent hack suffered by the platform.

As explained below in the article, the exact number of customer accounts impacted is 483.

Researchers had previously estimated the impact of hack to be anywhere between $15 and $33 million (https://www.theblockcrypto.com/post/130793/on-chain-analyst-claims-crypto-com-hack-was-closer-to-33-million). But, Marszalek stressed in the interview, "these numbers aren't particularly material and customer funds were never at risk."

> **Bloomberg Live**
> @BloombergLive
>
> JUST IN: CEO @cryptocom's Kris Marszalek discusses the site's recent hack with @BloombergTV's @emilychangtv. "Customer funds were never at risk." #TheYearAhead
>
> Watch on Twitter



In the same TV interview, Marszalek didn't directly answer the question, "what was behind this hack?" but did state that a postmortem was ongoing and that financial regulators hadn't yet reached out to the company.

Unauthorized withdrawals total $33.8 million

A statement from Crypto.com seen by BleepingComputer today puts the total amount of unauthorized withdrawals across different cryptocurrencies at approximately US**$34 million**.

Crypto.com unauthorized withdrawals

Amount withdrawn	Cryptocurrency	Amount in USD
4,836.26 ETH	Ethereum	$15,132,516
443.93 BTC	Bitcoin	$18,613,630
-	Miscellaneous	$66,200
Totals		$33,812,346

Crypto.com had first detected the cyber incident via its risk monitoring systems on January 17th, 2022, when "a small number of users had unauthorized crypto withdrawals on their accounts."

"Crypto.com promptly suspended withdrawals for all tokens to initiate an investigation and worked around the clock to address the issue," states (http://blog.crypto.com/crypto-com-security-report-next-steps/) the company.

Following the detection of the suspicious activity, the withdrawal infrastructure was shut down for approximately **14 hours** as a caution.

The platform additionally revoked two-factor authentication (2FA) tokens for its users, now prompting them to log back into the app and set up new 2FA tokens.

Although, at the time, many customers reported issues [1 (https://twitter.com/MarkSebulsky/status/1483097308459769857), 2 (https://twitter.com/Sparr0w_101/status/1483069373174665221), 3 (https://twitter.com/DodongdocM/status/1483111656334843906)] when attempting to follow the reset procedure.

"No customers experienced a loss of funds. In the majority of cases, we prevented the unauthorized withdrawal, and in all other cases customers were fully reimbursed... The incident affected 483 Crypto.com users."

Withdrawal transactions were resumed on January 18th, at around 5:46 PM UTC, according to the company, after additional "security hardening measures" were put in place.

It seems this isn't the first time the platform has suffered a technical issue.

In May 2021, BleepingComputer reported that a technical glitch led to duplicate purchases on the Crypto.com platform (https://www.bleepingcomputer.com/news/security/crypto-exchange-glitch-causes-duplicate-purchases-delayed-credits/)—with customers inadvertently spending two or three times the intended amount on cryptocurrency purchases, with no refunds issued.

At least, this time around, Crypto.com's customers haven't lost any funds as a result of unauthorized activity.

Related Articles:

US returns $154 Million in bitcoins stolen by Sony employee (https://www.bleepingcomputer.com/news/security/us-returns-154-million-in-bitcoins-stolen-by-sony-employee/)

QNAP warns users of bitcoin miner targeting their NAS devices (https://www.bleepingcomputer.com/news/security/qnap-warns-users-of-bitcoin-miner-targeting-their-nas-devices/)

The Week in Ransomware - December 3rd 2021 - Seizing Bitcoin (https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-3rd-2021-seizing-bitcoin/)

New BHUNT malware targets your crypto wallets and passwords (https://www.bleepingcomputer.com/news/security/new-bhunt-malware-targets-your-crypto-wallets-and-passwords/)

OpenSea NFT platform bugs let hackers steal crypto wallets (https://www.bleepingcomputer.com/news/security/opensea-nft-platform-bugs-let-hackers-steal-crypto-wallets/)