Crypto Threat Intelligence Report

3Commas API Data Breach

Executive Summary

Inca Digital's Scam and Fraud Intelligence API provides data for clients to identify parties involved in ransomware, phishing, extortion, pump & dumps, hack, theft, and other fraudulent events in the digital asset space.

The following report utilizes Inca Digital's data for an analysis of the 3Commas API fraud and provides evidence for law enforcement to complete the case. Inca Digital identified victims with a total loss of approximately $26 million. Based on our blockchain forensics work, Inca Digital estimates the actual monetary loss of the 3Commas API hack is close to $100 million.

COUNTRY/STATE/PROVINCE	Binance	Bittrex	Coinbase	KuCoin	Grand Total
Australia	$161,000			$45,000	$206,000
Belgium	$80,000				$80,000
Canada	$452,033			$24,593	$476,626
China				$9,000	$9,000
Czech republic	$20,000				$20,000
Egypt	$165,000				$165,000
European Union	$854,000				$854,000
France	$145,000				$145,000
Germany				$500	$500
Greece	$5,200				$5,200
Hong Kong	$96,578				$96,578
Kosovo	$275,000				$275,000
Latvia	$1,100,000				$1,100,000
Malaysia	$232,000				$232,000
Not Reported	$620,000			$26,900	$646,900
Portugal				$7,500	$7,500
Romania	$150,000				$150,000
Russia				$30,000	$30,000
Saudia Arabia				$80,000	$80,000
Singapore	$288,000			$125,772	$413,772
Slovenia	$60,000				$60,000
Spain	$81,000				$81,000
Thailand	$6,406,300			$1,400,000	$7,806,300
The Netherlands	$312,000			$4,500	$316,500
Turkey	$350,000			$25,000	$375,000
Ukraine	$810,000				$810,000
United Kingdom	$5,252,300		$200,000	$53,872	$5,506,172
United States	$107,158	$49,550	$1,859,569	$369,556	$2,385,833
Venezuela	$5,300				$5,300
Vietnam	$3,500,000				$3,500,000
Grand Total	**$21,527,869**	**$49,550**	**$2,059,569**	**$2,202,193**	**$25,839,181**

Total amount lost by victims that reported to Inca Digital

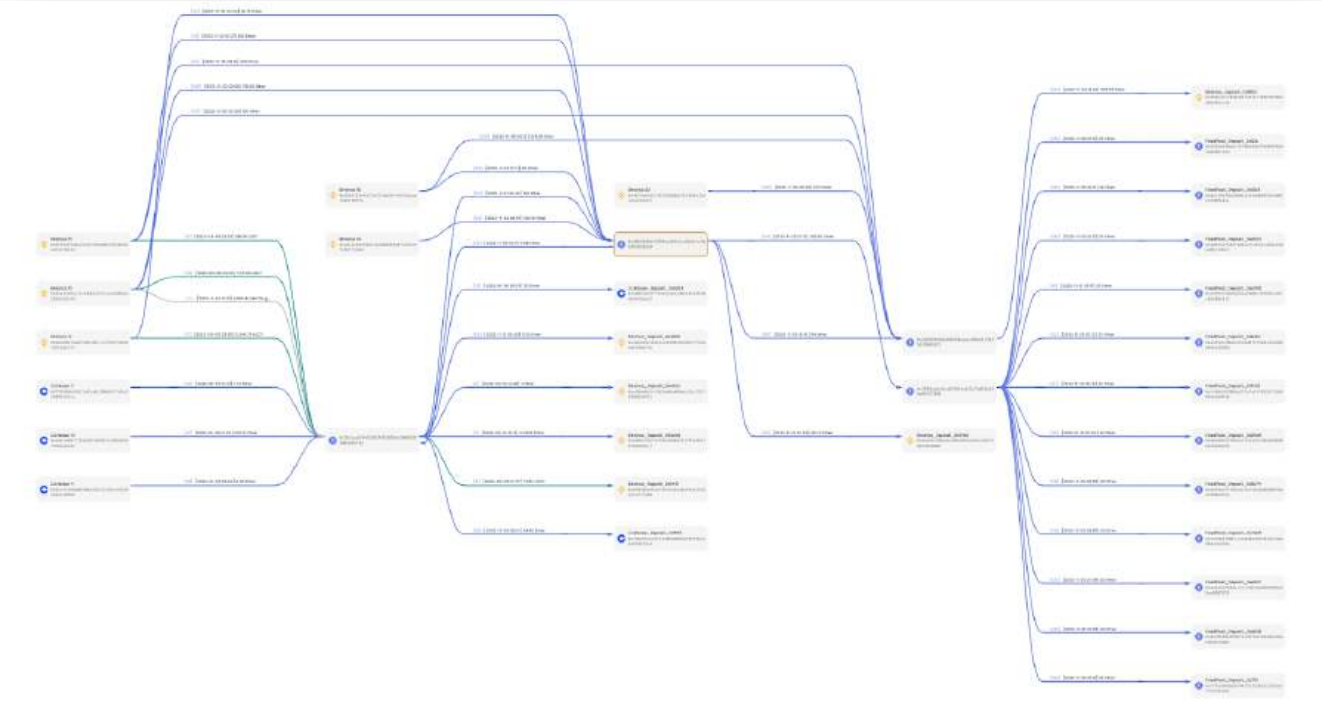
It is Inca Digital's assessment that the attack was not simply opportunistic individuals using leaked API keys as reported by 3Commas, but a sustained effort undertaken by a persistent cyber criminal threat.

The earliest evidence Inca Digital uncovered of the 3Commas hack is from late August 2022. The wallet addresses central to the network that conducted the 3Commas attacks have transaction history dating back to late 2021 using many of the Tactics, Techniques and Procedures (TTPs) notable for illicit financial transactions: incoming transactions mainly in ETH from centralized exchanges, use of decentralized exchanges to swap that ETH for stablecoins, and then a commingling of those stablecoins to similar addresses along the tracing. Further, price volatility peaks measured in the low liquidity markets used by the hackers indicate wash trading in those markets.

Trading pairs reported by victims on Binance and Coinbase – Price standard deviation peaks

Inca Digital's blockchain forensics work is ongoing and we anticipate discovering additional transaction records to add to this data set. In order to identify the perpetrators of the fraud, law enforcement will need to subpoena the centralized exchanges where the illicit trading took place, namely: Binance, Coinbase, KuCoin, and Bittrex, among others. Inca Digital has so far identified 418 transactions and 35 exchange wallet addresses of this type. In order to identify the further movement of the illicit funds which were withdrawn from those exchanges, law enforcement will need to subpoena FixedFloat, a non-custodial cryptocurrency exchange headquartered in Seychelles. Inca Digital has so far identified 153 transactions of this type.

Full data and evidence is available upon request.



Blockchain Wallet Forensics of 3Commas Hack