CHAINALYSIS IN ACTION

Chainalysis in Action: Department of Justice Announces Second-Largest Ever Crypto Seizure, with $3.36 Billion in Bitcoin Seized from Silk Road Hacker

SEPTEMBER 13, 2023 | BY CHAINALYSIS TEAM

In November 2021, IRS Criminal Investigations (IRS-CI) seized 50,676 Bitcoin from James Zhong, an American who pled guilty to wire fraud for stealing that Bitcoin from the darknet market Silk Road in September 2012. With a value of $3.36 billion, this marks one of the largest cryptocurrency seizures in history.

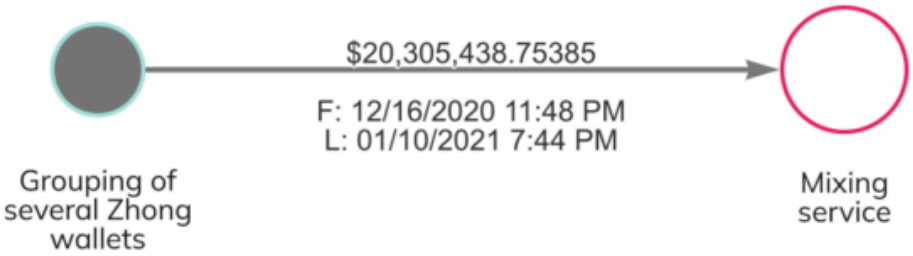
We commend the IRS-CI agents who led this investigation, as well as the DOJ lawyers who were able to achieve a guilty plea from Zhong. We're also proud to say that Chainalysis' own Aaron Bice assisted agents with the case, using Chainalysis Reactor and other proprietary tools to trace Zhong's attempts to launder the funds, and performing forensic database analysis to help agents identify Zhong and build their case against him. Below, we'll share more about Zhong's theft, money laundering strategy, and the investigation itself.

The hack of Silk Road, from theft to seizure

Active between 2011 and 2013, Silk Road was the first major crypto-powered darknet market, and at its peak accounted for over 20% of Bitcoin's daily economic activity. While Silk Road operator Ross Ulbricht was arrested in 2013, it wasn't until November 2021 that authorities would catch James Zhong, the person who stole 50,000 Bitcoin from the infamous darknet market in 2012.

Zhong pulled off the theft by exploiting a flaw in Silk Road's Bitcoin withdrawal mechanism for vendors. According to the Department of Justice (DOJ), Zhong set up fake Silk Road vendor accounts solely for this purpose, never actually listing anything for sale. Zhong funded the address associated with each vendor account with between 200 and 2,000 Bitcoin, and soon after would initiate multiple transactions to withdraw that amount in a matter of milliseconds. By doing this several times over several days, he was able to trick Silk Road's system into letting him withdraw more than he deposited, ultimately stealing 50,000 Bitcoin. We can see the results of this activity on the Chainalysis Reactor graph below.

Soon after the theft, Zhong consolidated his 50,000 Bitcoin in two wallets, with 40,000 Bitcoin in one and 10,000 in the other. The funds sat untouched for over a year, until he gradually moved them to new wallets over several years from October 2013 to May 2019. Between December 2020 and January 2021, Zhong also moved a portion of the funds to a mixing service in an effort to obfuscate the flow of funds.



We should also note that Zhong gained an additional 50,000 in Bitcoin Cash — the equivalent of his stolen Bitcoin holdings — when the Bitcoin Cash hard fork occurred in 2017. Soon after, Zhong exchanged that 50,000 Bitcoin Cash for 3,500 Bitcoin, bringing his total illicit holdings to 53,500 Bitcoin, a portion of which was also seized later.

Eventually, Zhong attempted to liquidate a portion of the stolen funds at a centralized cryptocurrency exchange in 2020. During that process, an address that had received funds directly from the Silk Road hack was included on the input side of a transaction along with an address easily traced to Zhong, allowing investigators to ascertain that Zhong controlled both. Additionally, the compliance team at that exchange provided law enforcement with the KYC information and IP address linked to the account associated with these transactions, which also led back to Zhong. Agents raided Zhong's Gainesville, Georgia home in November 2021, finding 50,491 Bitcoin on devices hidden in a floor safe and, on the lower end of Zhong's security measures, inside of a popcorn tin stuffed under blankets. Agents also turned up over $660,000 in cash, precious metals, and 25 Casascius coins, which are physical representations of Bitcoin containing private keys to access actual Bitcoin. Zhong voluntarily turned over another 861 Bitcoin in March 2022 and May 2022. In November 2022, he pled guilty to charges of wire fraud stemming from this theft, and was sentenced to just over a year in prison in April 2023.

Seizures are key in the fight against cryptocurrency-based crime

It should go without saying that no one has the right to steal money just because it was obtained through criminal activity. More importantly, this case shows how far law enforcement has progressed in its ability to follow and seize cryptocurrency associated with crime, even when criminals go to great lengths to hide it, and even when the activity in question occurred years in the past. The blockchain is forever, so investigators can always return to old, suspicious transactions and investigate them using the latest methods.

American law enforcement agencies — primarily IRS-CI but others as well — have now seized billions in digital assets, which should show would-be cybercriminals that cryptocurrency isn't the anonymous, untraceable asset they may hope it is. In fact, the immutable and public nature of blockchains means that cryptocurrency is usually easier to trace than fiat. We look forward to continuing our support of IRS-CI, the DOJ, and other law enforcement and prosecuting agencies around the world as they continue to progress in their ability to solve cryptocurrency-based crime.