Canadian national charged with stealing approximately $65 million in cryptocurrency from two DeFi protocols

Defendant exploited vulnerabilities in the KyberSwap and indexed finance decentralized finance protocols to steal from investors

February 10, 2025

The Joint Chiefs of Global Tax Enforcement (J5) welcomed the unsealing of an indictment in federal court this week charging a man with wire fraud, computer hacking and attempted extortion.

Andean Medjedovic is accused of stealing approximately $65 million in cryptocurrency from the KyberSwap and Indexed Finance decentralized finance (DeFi) protocols, which are sophisticated financial platforms residing on cryptocurrency blockchains. Medjedovic is also charged with laundering the proceeds of the theft. He is currently at large.

“As alleged, the defendant executed a highly sophisticated scheme to exploit two decentralized finance protocols and steal tens of millions of dollars’ worth of cryptocurrency from investors,” stated United States Attorney John J. Durham. “My Office remains at the forefront in prosecuting cutting-edge cases involving new and emerging technologies, demonstrating our commitment to protecting all financial markets, including the digital assets markets. Criminals like the defendant who take advantage of new technologies to harm investors will be held accountable no matter where in the world they carry out their schemes.”

“This was a sophisticated fraud that exploited vulnerabilities in ‘smart contracts’, resulting in the theft of millions of dollars in cryptocurrency,” said IRS-CI New York Special Agent in Charge Harry Chavis. “It’s alleged that Medjedovic executed a hack that stole nearly $65 million in crypto between two schemes, leaving liquidity pool investors in the red. In investigating this case, IRS-CI New York’s Cyber group worked closely with its federal partners while leveraging resources from IRS-CI’s Cyber Attaché at Europol and the J5 Cyber Group. Even with the complexities of DeFi, we tracked down who is responsible for this large-scale theft, and he is now a wanted man.”

KyberSwap and Indexed Finance were developers of automated marketmaking services called “liquidity pools” that allowed users to swap cryptocurrency tokens with each other. The liquidity pools were managed by computer code called “smart contracts” and relied on investor contributions of cryptocurrency. As alleged, Medjedovic used manipulative trading to exploit vulnerabilities in the KyberSwap and Indexed Finance smart contracts. These manipulative trades enabled Medjedovic to drain approximately $65 million in cryptocurrency that belonged to investors from the KyberSwap and Indexed Finance liquidity pools.

The KyberSwap Exploit

JUSTIN COLE JUSTIN.COLE@CI.IRS.GOV 202-768-2110

As alleged in the indictment, in 2023, Medjedovic planned and executed a scheme to exploit vulnerabilities in the KyberSwap protocol. KyberSwap was a DeFi protocol and developer of liquidity pools on several public blockchains, including the Ethereum and Arbitrum networks. Liquidity pools use user-contributed cryptocurrency to facilitate trading and market-making in cryptocurrencies. The KyberSwap liquidity pools were managed by computer code or "smart contracts" called automated market makers or "AMMs," which set prices in the KyberSwap liquidity pools.

In November 2023, Medjedovic exploited vulnerabilities in the KyberSwap computer code to drain the KyberSwap liquidity pools. Medjedovic used hundreds of millions of dollars in borrowed cryptocurrency to create artificial prices in the KyberSwap liquidity pools. Medjedovic then calculated precise combinations of trades that would cause the KyberSwap AMM to "glitch," in his words, allowing him to steal tens of millions of dollars in cryptocurrency from the liquidity pools. In total, Medjedovic stole approximately $48.8 million in investors' cryptocurrency from 77 KyberSwap liquidity pools on six public blockchains.

Following the exploit, Medjedovic attempted to extort the developers of the KyberSwap protocol, as well as KyberSwap's investors and the members of the decentralized autonomous organization or "DAO" that governed the KyberSwap protocol. Medjedovic demanded control of the KyberSwap protocol and the KyberSwap DAO in exchange for which he would return approximately 50% of the cryptocurrency that he had stolen.

Medjedovic also attempted to launder the proceeds of his theft, including through "bridge" protocols used to transfer cryptocurrency from one blockchain to another, and through a cryptocurrency "mixer" used to conceal the source of digital assets. After one bridge protocol froze several of his transactions, Medjedovic agreed to pay an undercover law enforcement agent posing as a software developer approximately $80,000 to circumvent the bridge protocol's restrictions and release approximately $500,000 in stolen cryptocurrency.

The Indexed Finance Exploit

As alleged in the indictment, Medjedovic committed a similar exploit of the Indexed Finance DeFi protocol. Indexed Finance liquidity pools are referred to as "index pools," and function similarly to a mutual fund or exchange-traded fund in traditional finance. Instead of holding a basket of traditional equities, the index pools held an index of digital tokens contributed by users.

In October 2021, Medjedovic used manipulative trading to exploit two Indexed Finance liquidity pools on the Ethereum network. Medjedovic used hundreds of millions of dollars in borrowed cryptocurrencies to distort a process called "re-indexing," which was used by the Indexed Finance smart contracts to add a new token to the liquidity pools. Medjedovic used the borrowed cryptocurrency to engage in manipulative trading to cause the Indexed Finance smart contracts to set artificial prices during the reindexing process. He then stole approximately $16.5 million in investor cryptocurrency from the liquidity pools.

Beginning after the Indexed Finance exploit, in or around 2022, Medjedovic conspired with another person to launder the proceeds of his illegal conduct through cryptocurrency exchange accounts that were opened using false information, and by using a cryptocurrency mixer. Among other things, Medjedovic maintained a step-bystep playbook for moving large amounts of cryptocurrency through the mixer, which he titled a "moneyMovementSystem." In other documents, Medjedovic discussed circumventing "know your customer" or "KYC" procedures and using cryptocurrency exchange accounts opened with false KYC information for "hacks and cashing out."

Valuable assistance was provided by the Justice Department's Office of International Affairs. The Office thanks the Netherlands' Public Prosecution Service and the Dutch National Police's Cybercrime Unit in The Hague and United States Customs and Border Protection, New York Field Office.

The J5 works together to gather information, share intelligence and conduct coordinated operations against transnational financial crimes. The J5 includes the Australian Taxation Office, the Canada Revenue Agency, the Dutch Fiscal Intelligence and Investigation Service, His Majesty's Revenue and Customs from the U.K. and IRS-CI from the U.S.

For more information about the J5, please visit www.irs.gov/j5.

JUSTIN COLE JUSTIN.COLE@CI.IRS.GOV 202-768-2110