Russian man pleads guilty to laundering Ryuk ransomware money

By Sergiu Gatlan

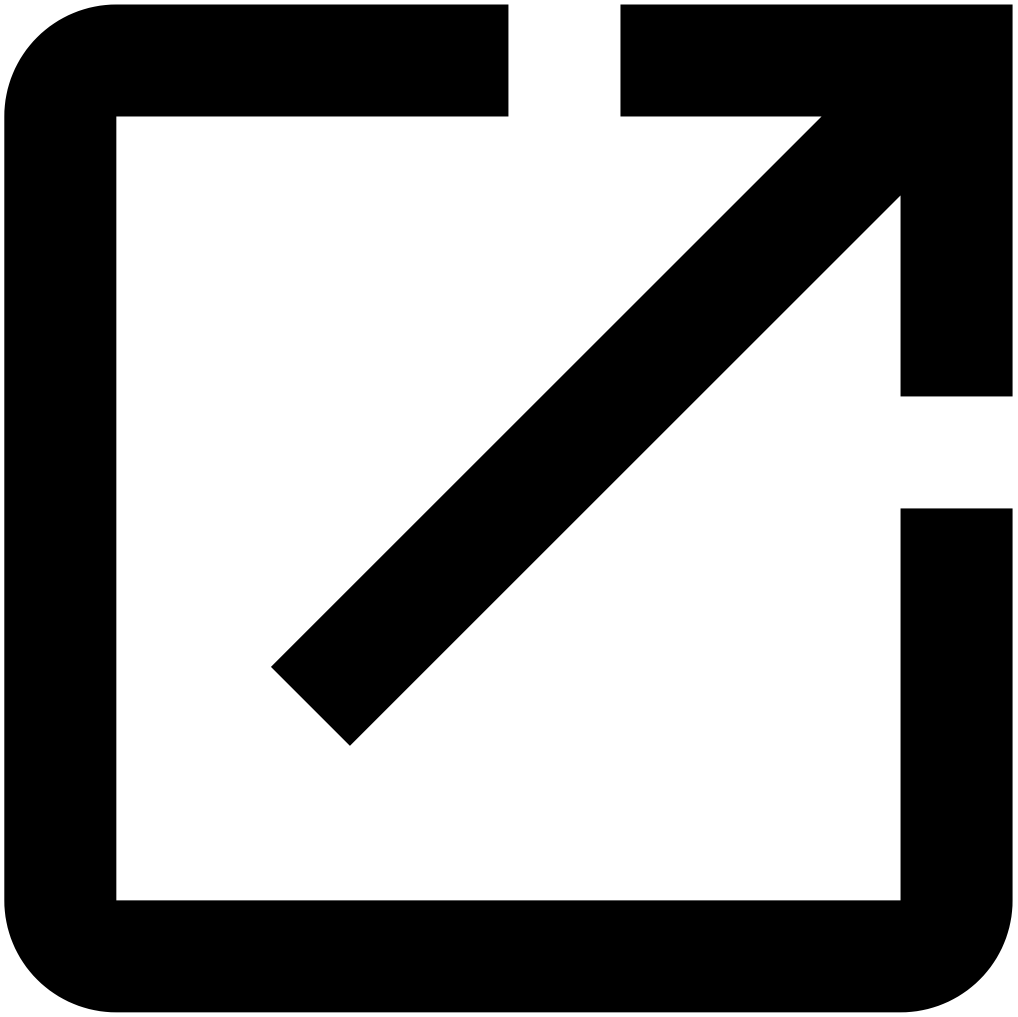
Published: 2023-02-07 · Archived: 2026-04-05 15:14:24 UTC

Russian citizen Denis Mihaqlovic Dubnikov pleaded guilty on Tuesday to laundering money for the notorious Ryuk ransomware group for over three years.

The guilty plea comes after Dubnikov, a former crypto-exchange executive and the co-founder of crypto trading platforms Coyote Crypto and Eggchange, was arrested in Amsterdam in November 2021 and extradited to the United States in August 2022.

He made his first appearance in a U.S. federal court in Portland one day after the extradition date, on August 17, 2022.


DIE LINKE.
0:00

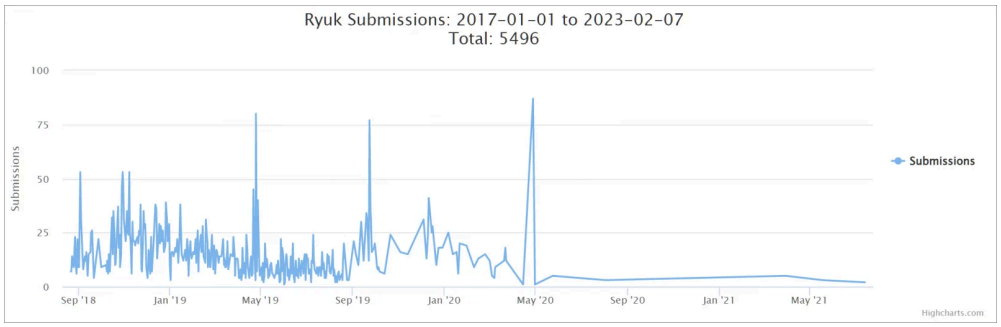


From August 2018 to August 2021, Dubnikov and 13 other accomplices participated in money laundering activities involving proceeds from Ryuk ransomware attacks targeting individuals and organizations in the United States and worldwide.

The money laundering group, including Dubnikov, used various financial transactions, including international ones, to hide the origin, location, and identity of those who received the ransom payments.

Ryuk is a former ransomware-as-a-service (RaaS) operation active between August 2018 and the middle of 2020, when the Wizard Spider cybercrime group behind it switched to Conti ransomware.

Conti also shut down operations in May 2022, when it rebranded into multiple smaller units that either launched new operations or infiltrated existing ransomware gangs.



Ryuk ransomware submissions (ID Ransomware)

Dubnikov laundered Ryuk ransom paid by US company

According to a superseding indictment, after victims paid the Ryuk ransoms in the form of bitcoin to private wallets, the co-conspirators involved in the money laundering scheme divided the payments into smaller amounts. Then they transferred the ransoms to various other private wallets.

The criminal group used hundreds of private wallets to carry out these transactions, each with thousands of associated public keys.

They then moved some of the bitcoin from the private wallets to cryptocurrency exchange accounts where the bitcoin was exchanged for Tether, other cryptocurrencies, or fiat currency.

The Ryuk ransom proceeds (exchanged into Tether or another cryptocurrency) were then sent to other conspirators' accounts at other cryptocurrency exchanges to be exchanged for fiat currency (usually Chinese Renminbi) using those exchanges' "over the counter" services.

"Specifically, in July 2019, a United States-based company paid a 250 Bitcoin Ryuk ransom after a ransomware attack. On or about July 11, 2019, in Moscow, Russia, Dubnikov accepted 35 Bitcoin from a co-conspirator in exchange for approximately $400,000," the Department of Justice said in a press release issued today.

"The Bitcoin transferred to Dubnikov were directly sourced from the ransom paid by the American company. Dubnikov converted the Bitcoin to Tether and sent it to a second co-conspirator, who eventually exchanged it for Chinese Renminbi."

If found guilty, Dubnikov can get a sentence of up to 20 years of federal imprisonment, three years of supervised release, and a fine of up to $500,000. The defendant will be sentenced on April 11, 2023.

Source: https://www.bleepingcomputer.com/news/security/russian-man-pleads-guilty-to-laundering-ryuk-ransomware-money/