Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 million from Ransomware Attackers, Scammers, and Darknet Markets

blog.chainalysis.com/reports/ofac-sanction-suex-september-2021

Chainalysis Team

September 22, 2021

Want to learn more about the sanctions against Suex and what this means for the larger fight against ransomware? Watch Chainalysis investigators and U.S. Treasury executives discuss the Suex investigation and new OFAC guidance on sanctions risk for ransomware payments now.

Today, the U.S. Treasury's Office of Foreign Assets Control (OFAC) announced that Russia-based cryptocurrency Over The Counter (OTC) broker Suex was designated pursuant to Executive Order 13694 and added to the Specially Designated Nationals and Blocked Persons (SDN) List, thereby prohibiting Americans from doing business with the company. We are proud to share that Chainalysis tools aided in the investigation of Suex.

Since opening its doors in 2018, Suex has moved hundreds of millions of dollars worth of cryptocurrency, mostly in Bitcoin, Ether, and Tether, much of which is from illicit and high-risk sources. In Bitcoin alone, Suex's deposit addresses hosted at large exchanges have received over $160 million from ransomware actors, scammers, and darknet market operators. Chainalysis' investigation reveals that the OTC is converting cryptocurrency into cash at physical branches located in Moscow and St. Petersburg, and possibly also at other offices outside of Russia as well. Suex is also found to have received over $50 million worth of Bitcoin sent from addresses hosted at illicit cryptocurrency exchange BTC-e from 2018 through 2021, well after BTC-e was shut down by U.S. authorities for its own money laundering activity on behalf of cybercriminals.

Chainalysis has been tracking Suex's money laundering activity for some time now. Following this investigation, we can reveal that multiple Suex addresses are included in the group of 273 service deposit addresses we identified as receiving 55% of all funds sent from illicit addresses in 2020 in our most recent Crypto Crime Report. Suex addresses also appear in the Rogue 100, a list of 100 OTC deposit addresses we identified as belonging to major money laundering facilitators in 2019.

Today's designation is important because it represents significant action taken by the U.S. government to combat the money launderers who make all other forms of cryptocurrency-based crime profitable. As we discussed in our most recent Crypto Crime Report, a very small group of illicit services facilitates the majority of the money laundering for all cryptocurrency-based crime. Suex is one of the biggest and most active of those services. Shutting them down would represent a significant blow to many of the biggest cyber threat actors operating today, including leading ransomware attackers, scammers, and darknet market operators.

Who is Suex?

Suex is a cryptocurrency OTC broker legally registered in the Czech Republic. However, it has no known physical presence there and instead operates out of branch offices in Moscow and St. Petersburg, as well as other locales in and around Russia and in the Middle East. Suex claims it can convert cryptocurrency holdings into cash at these branch locations and even facilitate the exchange of cryptocurrency for physical assets like real estate, cars, and yachts.

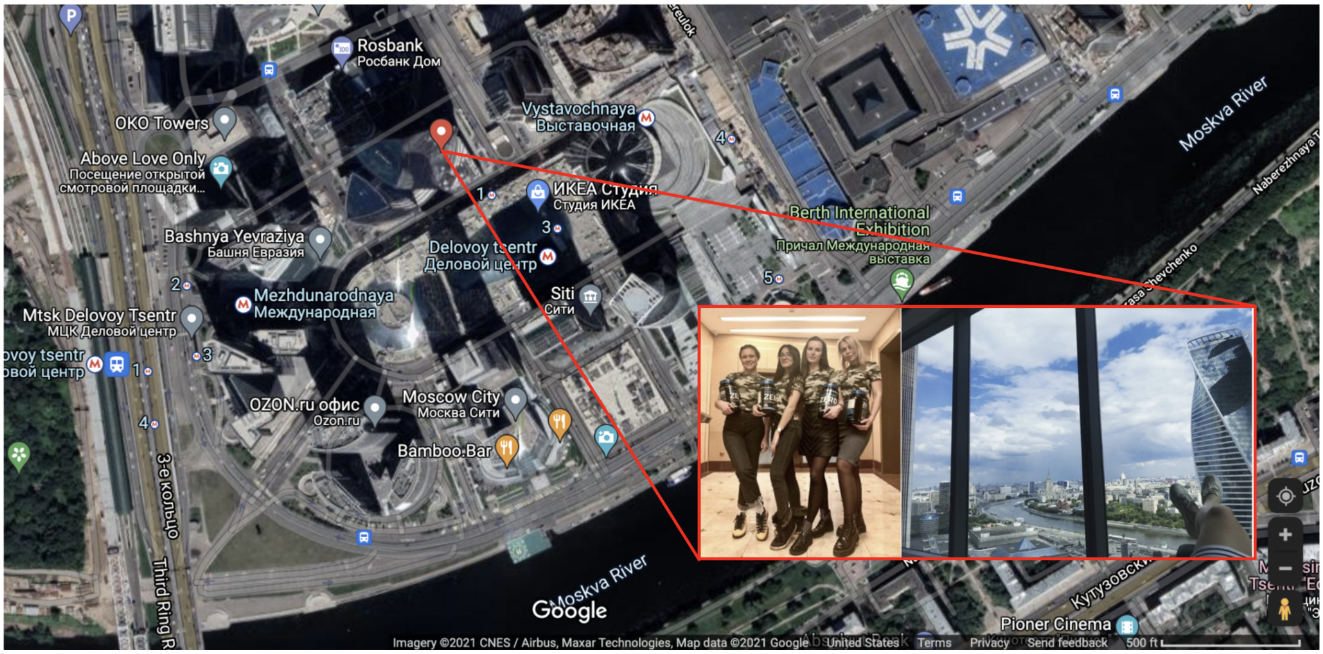


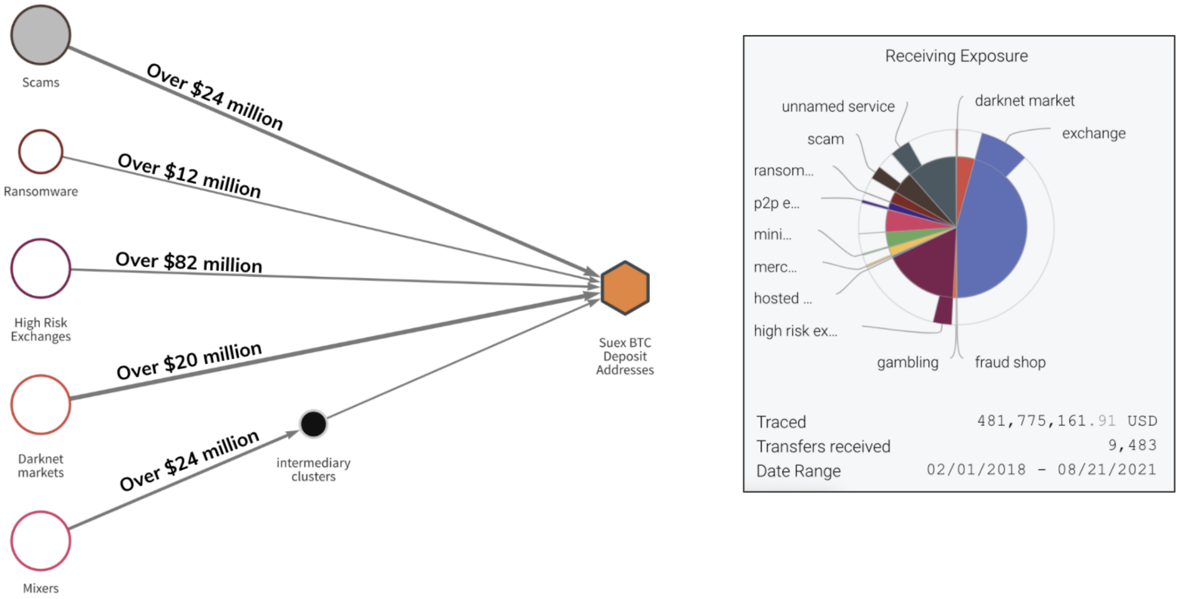
Photo (L) of alleged Suex employees at elevator bank at reported Suex office location at 12 Federation East Tower, Moscow City, Moscow and photo (R) reportedly taken within the Suex office suite (map courtesy of Google Maps).

Suex’s blockchain footprint

Suex operates as a nested service, meaning it operates using addresses hosted by larger exchanges in order to tap into those exchanges’ liquidity and trading pairs. While many nested services are legitimate, some exchanges don’t hold nested services to high enough compliance standards, meaning they can be exploited for money laundering.

Blockchain analysis reveals that Suex has received tens of millions worth of cryptocurrency payments from addresses associated with several forms of cybercrime, as well as from addresses associated with the now-shuttered exchange BTC-e. While Suex’s activity spanned several cryptocurrencies, we’ll dive more into its Bitcoin transaction history below using Chainalysis Reactor.

Suex has received over $160 million in BTC from illicit and high-risk sources since 2018

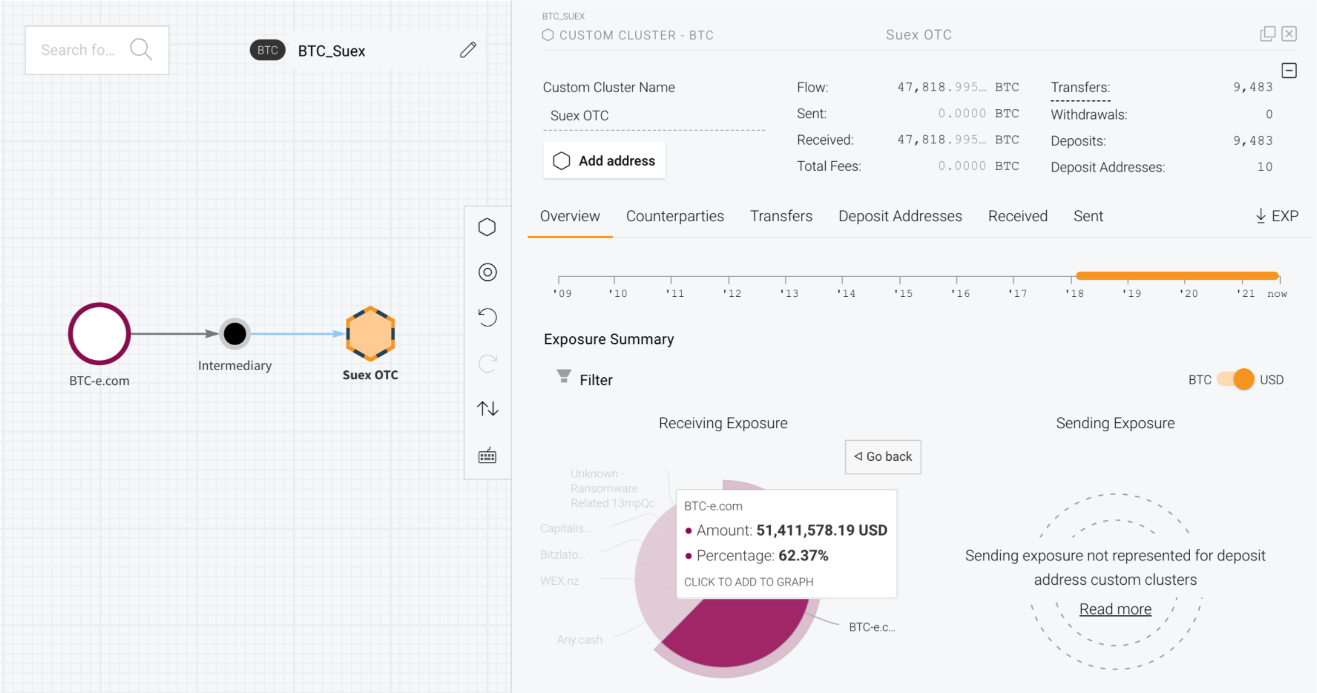


Traced 481,775,161.91 USD
Transfers received 9,483
Date Range 02/01/2018 - 08/21/2021

Suex has received over $481 million in Bitcoin alone since becoming active in February 2018, based on the value at the time of transfers. Those transfers include substantial funds received from cybercriminals. Specifically, Suex has received:

- Nearly $13 million from **ransomware operators** including Ryuk, Conti, Maze, and several others
- Over $24 million from **cryptocurrency scam operators** including the fraudsters behind Finiko, a scam that took in over $1 billion worth of cryptocurrency from victims primarily in Russia and Ukraine
- Over $20 million from **darknet markets**, primarily the Russia-based Hydra Market

Additionally, Suex received over $50 million worth of cryptocurrency from addresses associated with BTC-e, an illicit cryptocurrency exchange shut down by authorities in 2017 for facilitating large-scale money laundering on behalf of cybercriminals.



BTC_SUEX

CUSTOM CLUSTER - BTC Suex OTC

Custom Cluster Name: Suex OTC

Flow:	47,818.995… BTC	Transfers:	9,483
Sent:	0.0000 BTC	Withdrawals:	0
Received:	47,818.995… BTC	Deposits:	9,483
Total Fees:	0.0000 BTC	Deposit Addresses:	10

Exposure Summary

BTC-e.com
- Amount: **51,411,578.19 USD**
- Percentage: **62.37%**

CLICK TO ADD TO GRAPH

Sending exposure not represented for deposit address custom clusters

Interestingly, the transfers from BTC-e to Suex took place well after BTC-e was shuttered, with some occurring as recently as this year. We believe Suex may have processed these transfers on behalf of BTC-e administrators, associates, or former users attempting to liquidate cryptocurrency trapped at the exchange. Our analysis of Suex's blockchain activity combined with proprietary investigative techniques suggests to us that the OTC carried out cryptocurrency-for-cash exchanges on behalf of users at its Moscow and St. Petersburg branch locations, but possibly at others as well.

Suex cryptocurrency addresses named in the OFAC SDN listing

The following Suex cryptocurrency addresses were named in OFAC's SDN designation against the OTC broker:

- 12HQDsicffSBaYdJ6BhnE22sfjTESmmzKx (BTC)
- 1L4ncif9hh9TnUveqWq77HfWWt6CJWtrnb (BTC)
- 13mnk8SvDGqsQTHbiGiHBXqtaQCUKfcsnP (BTC)
- 1Edue8XZCWNoDBNZgnQkCCivDyr9GEo4x6 (BTC)
- 1ECeZBxCVJ8Wm2JSN3Cyc6rge2gnvD3W5K (BTC)
- 1J9oGoAiHeRfeMZeUnJ9W7RpV55CdKtgYE (BTC)
- 1295rkVyNfFpqZpXvKGhDqwhP1jZcNNDMV (BTC)
- 1LiNmTUPSJEd92ZgVJjAV3RT9BzUjvUCkx (BTC)
- 1LrxsRd7zNuxPJcL5rttnoeJFy1y4AffYY (BTC)
- 1KUUJPkyDhamZXgpsyXqNGc3x1QPXtdhgz (BTC)

- 1CF46Rfbp97absrs7zb7dFfZS6qBXUm9EP (BTC)
- 1Df883c96LVauVsx9FEgnsourD8DELwCUQ (BTC)
- Bc1qdt3gml5z5n50y5hm04u2yjdphefkm0fl2zdj68 (BTC)
- 1B64QRxfaa35MVkf7sDjuGUYAP5izQt7Qi (BTC)
- 0x2f389ce8bd8ff92de3402ffce4691d17fc4f6535 (ETH)
- 0x19aa5fe80d33a56d56c78e82ea5e50e5d80b4dff (ETH)
- 0xe7aa314c77f4233c18c6cc84384a9247c0cf367b (ETH)
- 0x308ed4b7b49797e1a98d3818bff6fe5385410370 (ETH)
- 0x2f389ce8bd8ff92de3402ffce4691d17fc4f6535 (USDT)
- 0x19aa5fe80d33a56d56c78e82ea5e50e5d80b4dff (USDT)
- 1KUUJPkyDhamZXgpsyXqNGc3x1QPXtdhgz (USDT)
- 1CF46Rfbp97absrs7zb7dFfZS6qBXUm9EP (USDT)
- 1LrxsRd7zNuxPJcL5rttnoeJFy1y4AffYY (USDT)
- 1Df883c96LVauVsx9FEgnsourD8DELwCUQ (USDT)
- 16iWn2J1McqjToYLHSsAyS6En3QA8YQ91H (USDT)

Chainalysis has labeled these addresses in all of our products as being associated with a sanctioned entity and today will be alerting any customers with any exposure to these addresses.

A big win in the fight against money laundering

Shutting down cryptocurrency-based money launderers is one of the most important strategies to combat cryptocurrency-related crime. It all comes down to incentives. If cybercriminals have no way of moving ill-gotten cryptocurrency to services where it can be stored safely or converted into cash, there’s much less reason for them to use cryptocurrency in the first place. A small group of illicit services facilitate the majority of cryptocurrency-based money laundering, and Suex is one of the worst offenders, so today’s action represents a positive step forward in the fight against cybercrime. We commend OFAC for making this designation and look forward to working with our partners in the public and private sectors to continue the fight against money laundering service providers.

Want to learn more about the sanctions against Suex and what this means for the larger fight against ransomware? Watch Chainalysis investigators and U.S. Treasury executives discuss the Suex investigation and new OFAC guidance on sanctions risk for ransomware payments now.