

US sanctions crypto exchange over ransomware ties

21 September 2021, by Joshua Melvin



Washington has announced sanctions against a cryptocurrency exchange it says has worked with ransomware attackers.

The United States imposed sanctions Tuesday on cryptocurrency exchange SUEX for its ties to ransomware extortionists, as Washington seeks to crack down on a sharp rise in digital crime attacks.

The move marks the first US sanctions against a virtual currency exchange and they come as President Joe Biden's administration has been under pressure to act after high-profile hacks and data breaches.

The attacks on a major US oil pipeline, a meatpacking company and Microsoft Exchange email system caused real-world problems and drew attention to the vulnerability to US infrastructure to digital pirates.

The US Treasury Department, which announced the sanctions, did not say if SUEX was implicated in any of those incidents, but noted that 40 percent of the exchange's known transaction history was linked to "illicit actors."

"Some virtual currency exchanges are exploited by malicious actors, but others, as is the case with SUEX, facilitate illicit activities for their own illicit gains," a Treasury statement said, adding they are the first sanctions against a crypto exchange.

As a result of the sanctions, any assets of the platform under US jurisdiction are now blocked and Americans are barred from using SUEX.

\$10 million reward

Crypto experts from Chainalysis noted large sums had moved through the platform, much of it from suspect 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," said a report from Chainalysis, which provides data on cryptocurrency.

SUEX is registered in the Czech Republic, and has branches in Russia and the Middle East.

Chainalysis said the US designation is important because it "represents significant action" by Washington to combat the money laundering that is key to digital crime.

The United States also issued a fresh warning against companies and individuals paying ransoms to unlock their files seized by ransomware hackers.

It noted that Americans could face penalties themselves if they are involved in making ransom payments as the United States already has a blacklist of people and countries, some of which are linked to ransomware attacks.

Tuesday's announcement comes after Washington in July offered \$10 million rewards for information on online extortionists abroad as it stepped up efforts to halt a sharp rise in ransomware attacks.

This year has seen a slew of prominent [ransomware](#) attacks which have disrupted a US pipeline, a meat processor and the software firm Kaseya—affecting 1,500 businesses, many of them far from the limelight.

Some \$350 million was paid to malicious cyber actors last year, a spike of 300 percent from 2019, according to the Department of Homeland Security.

US officials say many of the attacks originate in Russia although they have debated to what extent there is state involvement. Russia denies responsibility.

© 2021 AFP

APA citation: US sanctions crypto exchange over ransomware ties (2021, September 21) retrieved 28 January 2022 from <https://techxplore.com/news/2021-09-sanctions-crypto-exchange-ransomware-ties.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.