FiveBy

ALERT

08 November 2021

Treasury Sanctions Ransomware Operators and Another Virtual Currency Exchange; Issues Updated Ransomware Advisory

The Treasury Department's Office of Foreign Assets Control (OFAC) this week designated two ransomware operators and a virtual currency exchange, while the Financial Crimes Enforcement Network (FinCEN), in connection with the new designations, issued an updated ransomware advisory about the use of the US financial system to facilitate ransom payments.

The Justice Department this week has also announced charges against two foreign nationals, who allegedly deployed the Sodinokibi/REvil ransomware against businesses and US government entities. The department seized $6.1 million traceable to alleged ransom payments received by one of the sanctioned individuals, Yevgeniy Polyanin, and arrested Ukrainian national Yaroslav Vasinsky for conducting ransomware attacks, including the attack against IT software company Kaseya in July. Two additional Sodinokibi/REvil actors have been arrested in Romania. Meanwhile, the State Department is offering a Transnational Organized Crime Reward offer of up to $10,000,000 for information leading to the identification or location of any individual(s) who hold a key leadership position in the Sodinokibi/REvil group and up to $5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a Sodinokibi variant ransomware incident.

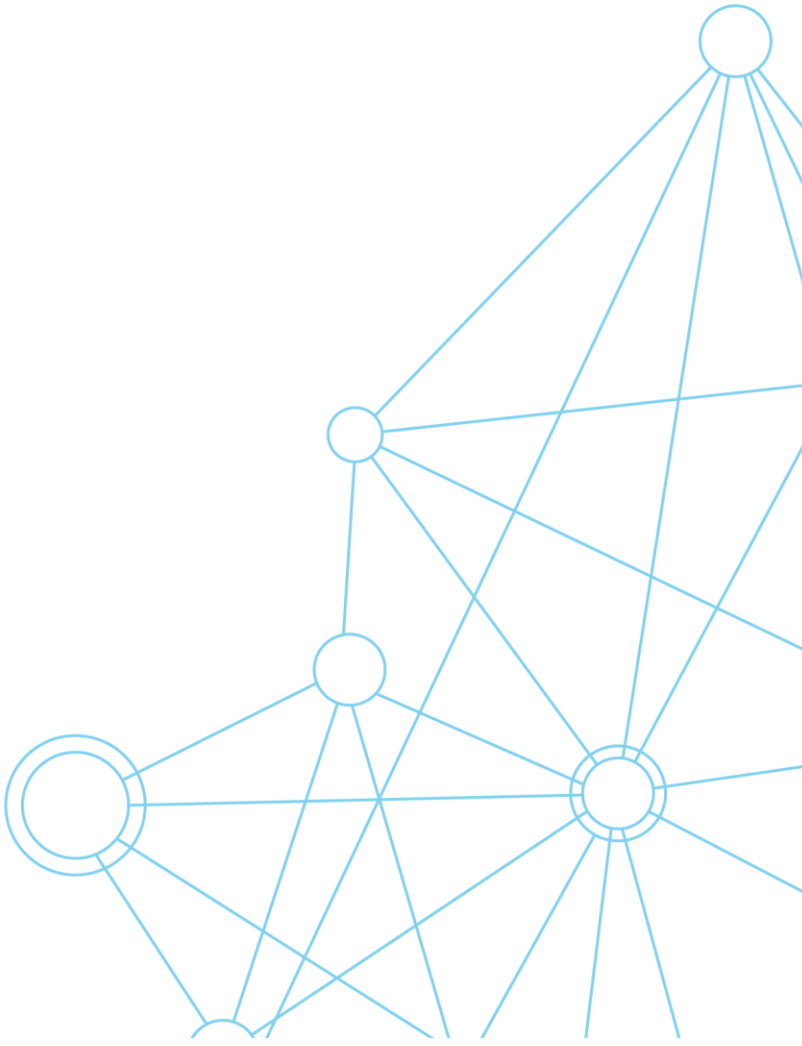
The coordinated effort shows the Biden administration's whole-of-government approach to combating ransomware and the focus on collaboration with foreign partners, as highlighted in Treasury's recent sanctions review. But more than that, the organized action demonstrates the Biden administration's commitment to engaging with the private sector partners for support and technology tools to ensure that cyber criminals are held accountable for their crimes. The Justice Department's arrest of Vasinsky and charges against both him and Polyanin, as well as the trace of the funds linked to alleged ransom payments, was the result of cooperation between the US government, foreign partners, and private-sector companies such as Microsoft, BitDefender, and McAfee.

In September, OFAC issued its first designation against the SUEX cryptocurrency exchange—a nested exchange registered in Czechia but based in Russia, which uses accounts at major global cryptocurrency exchanges to provide services to its clients and allow them to conduct virtual currency transactions. Chatex, the entity designated this week, is closely linked with SUEX, and more than half of its transactions are connected with illicit or high-risk activities, including ransomware. Chatex also provides material support to SUEX, and three other companies—IZIBITS OU, Chatextech SIA, and Hightrade Finance Ltd.—are designated for providing material support to Chatex.

FinCEN's updated advisory reflects the growing proliferation of anonymity-enhanced cryptocurrencies and decentralized mixers and highlights the role of decentralized exchanges, and sometimes, digital forensic and incident response companies and cyber insurance firms in facilitating the movement of virtual currencies in ransomware attacks. FinCEN also highlights two additional trends—the use of unregistered virtual currency mixing services and the use of foreign cash-out services that have insufficient compliance controls or operate in jurisdictions with lax regulatory oversight—as potential indicators of risk. It also adds two new red flags to its guidance, including the use of encrypted routers or networks and transferring funds using a mixing service.

INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM

This week's designations and coordinated actions stress the Biden administration's focus on ensuring that individuals and firms that facilitate ransomware payments and the movements of illicit transactions—whether virtually or through the global financial system—are held accountable through criminal prosecutions, sanctions, and other regulatory measures. These actions are also a continued warning to US firms in the virtual currency space to prepare for additional scrutiny and use all available tools to ensure compliance with US sanctions prevent transactions with actors linked to ransomware and other malign cyber activities.



INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM