

Treasury Takes Robust Actions to Counter Ransomware

September 21, 2021

Targets First Virtual Currency Exchange for Laundering Cyber Ransoms

OFAC Updates Ransomware Advisory to Encourage Reporting and Cyber Resilience

WASHINGTON — As part of the whole-of-government effort to counter ransomware, the U.S. Department of the Treasury today announced a set of actions focused on disrupting criminal networks and virtual currency exchanges responsible for laundering ransoms, encouraging improved cyber security across the private sector, and increasing incident and ransomware payment reporting to U.S. government agencies, including both Treasury and law enforcement. Treasury's actions today advance the United States government's broader counter-ransomware strategy, which emphasizes the need for a collaborative approach to counter ransomware attacks, including partnership between the public and private sector and close relationships with international partners.

“Ransomware and cyber-attacks are victimizing businesses large and small across America and are a direct threat to our economy. We will continue to crack down on malicious actors,” said Treasury Secretary Janet L. Yellen. “As cyber criminals use increasingly sophisticated methods and technology, we are committed to using the full range of measures, to include sanctions and regulatory tools, to disrupt, deter, and prevent ransomware attacks.”

Ransomware attacks are increasing in scale, sophistication, and frequency, victimizing governments, individuals, and private companies around the world. In 2020, ransomware payments reached over \$400 million, more than four times their level in 2019. The U.S. government estimates that these payments represent just a fraction of the economic harm caused by cyber-attacks, but they underscore the objectives of those who seek to weaponize technology for personal gain: to disrupt our economy and damage the companies, families, and individuals who depend on it for their livelihoods, savings, and futures. In addition to the millions of dollars paid in ransoms and recovery, the disruption to critical sectors, including financial services, healthcare, and energy, as well as the exposure of confidential information, can cause severe damage.

Some virtual currency exchanges are a critical element of this ecosystem, as virtual currency is the principal means of facilitating ransomware payments and associated money laundering activities. The United States has been a leader in applying its anti-money laundering/countering the financing of terrorism (AML/CFT) framework in the virtual currency area, including with the Financial Crimes Enforcement Network (FinCEN) publishing guidance regarding the application of Bank Secrecy Act rules in this area in 2013 and 2019. FinCEN has also taken important enforcement action against non-compliant virtual currency money transmitters facilitating ransomware payments, such as BTC-e in 2017 and the virtual currency mixing service Helix in 2020. In addition, the United States is taking steps to improve transparency regarding ransomware attacks and associated payments.

DESIGNATION OF FIRST VIRTUAL CURRENCY EXCHANGE FOR COMPLICIT FINANCIAL SERVICES

Today's actions include the Department of the Treasury's Office of Foreign Assets Control's (OFAC) designation of SUEX OTC, S.R.O. (SUEX), a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors. SUEX has facilitated transactions involving illicit proceeds from at least eight ransomware variants. Analysis of known SUEX transactions shows that over 40% of SUEX's known transaction history is associated with illicit actors. SUEX is being designated pursuant to Executive Order 13694, as amended, for providing material support to the threat posed by criminal ransomware actors.

Virtual currency exchanges such as SUEX are critical to the profitability of ransomware attacks, which help fund additional cybercriminal activity. Treasury will continue to disrupt and hold accountable these entities to reduce the incentive for cybercriminals to continue to conduct these attacks. This action is the first sanctions designation against a virtual currency exchange and was executed with assistance from the Federal Bureau of Investigation.


While most virtual currency activity is licit, virtual currencies can be used for illicit activity through peer-to-peer exchangers, mixers, and exchanges. This includes the facilitation of sanctions evasion, ransomware schemes, and other cybercrimes. 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. Treasury will continue to use its authorities against malicious cyber actors in concert with other U.S. departments and agencies, as well as our foreign partners, to disrupt financial nodes tied to ransomware payments and cyber-attacks. Those in the virtual currency industry play a critical role in implementing appropriate

AML/CFT and sanctions controls to prevent sanctioned persons and other illicit actors from exploiting virtual currencies to undermine U.S. foreign policy and national security interests.

SANCTIONS IMPLICATIONS

As a result of today's designation, all property and interests in property of the designated target that are subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Additionally, any entities 50% or more owned by one or more designated persons are also blocked. In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions or be subject to an enforcement action. Today's action against SUEX does not implicate a sanctions nexus to any particular Ransomware-as-a-Service (RaaS) or variant.

OFAC UPDATES ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS

OFAC today also released an [Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments](#) . The Advisory emphasizes that the U.S. government continues to strongly discourage the payment of cyber ransom or extortion demands and recognizes the importance of cyber hygiene in preventing or mitigating such attacks. OFAC has also updated the Advisory to emphasize the importance of improving cybersecurity practices and reporting to, and cooperating with, appropriate U.S. government agencies in the event of a ransomware attack. Such reporting, as the Advisory notes, is essential for U.S. government agencies, including law enforcement, to understand and counter ransomware attacks and malicious cyber actors.

OFAC strongly encourages victims and related companies to report these incidents to and fully cooperate with law enforcement as soon as possible to avail themselves of OFAC's significant mitigation related to OFAC enforcement matters and receive voluntary self-disclosure credit in the event a sanctions nexus is later determined.

ADDITIONAL AUTHORITIES

FinCEN, in addition to the guidance and enforcement activities above, has also engaged with industry, law enforcement, and others on the ransomware threat through the FinCEN Exchange public-private partnership. FinCEN held a first Exchange on ransomware in

November 2020 and a second Exchange in August 2021. FinCEN is taking additional action under its authorities to collect information relating to ransomware payments.

INTERNATIONAL COOPERATION AND IMPORTANCE OF AML/CFT MEASURES FOR VIRTUAL CURRENCIES AND SERVICE PROVIDERS

Countering ransomware benefits from close collaboration with international partners. At the Group of Seven (G7) meeting in June, participants committed to working together to urgently address the escalating shared threat from criminal ransomware networks. The G7 is considering the risks surrounding ransomware, including potential impacts to the finance sector. For example, the G7 Cyber Expert Group (CEG), co-chaired by Treasury and Bank of England, met on September 1 and September 14, 2021 to discuss ransomware, which remains a grave concern given the number and breadth of ransomware attacks across industry sectors. The participants considered the effects of ransomware attacks on the financial services sector, as well as the broader economy, and explored ways to help improve overall security and resilience against malicious cyber activity.

Given the illicit finance risk that virtual assets pose, including ransomware-related money laundering, in June 2019 the Financial Action Task Force (FATF) amended its standards to require all countries to regulate and supervise virtual asset service providers (VASPs), including exchanges, and to mitigate against such risks when engaging in virtual asset transactions. Among other things, countries are expected to impose customer due diligence (CDD) requirements, and suspicious transaction reporting obligations across VASPs, which can help inhibit cybercriminals' exploitation of virtual assets while supporting investigations into these illicit finance activities. Because profit-motivated cybercriminals must launder their misappropriated funds, AML/CFT regimens are a critical chokepoint in countering and deterring this criminal activity. This magnifies the need for all countries to effectively and expeditiously implement and enforce the FATF's standards on virtual assets and VASPs. The United States is committed to continued work at the FATF and with other countries to implement the FATF standards, and we welcome the FATF's ongoing work on this issue.

Click [here](#) to view identifying information on the entity designated today.

Click [here](#) for OFAC's Frequently Asked Questions on Virtual Currency.

FOR MORE INFORMATION ON RANSOMWARE

Please visit [StopRansomware.gov](https://stopransomware.gov), a one-stop resource for individuals and organizations of all sizes to reduce their risk of ransomware attacks and improve their cybersecurity resilience. This webpage brings together tools and resources from multiple federal government agencies under one online platform. Learn more about how ransomware works, how to protect yourself, how to report an incident, and how to request technical assistance.

###