Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange

November 8, 2021

FinCEN Updates Ransomware Advisory

OFAC Sanctions Two Ransomware Operators and a Virtual Currency Exchange Network for the Kaseya Incident and Laundering Cyber Ransoms

WASHINGTON — Continuing the Administration's whole-of-government effort to counter ransomware, the U.S. Department of the Treasury today announced a set of actions focused on disrupting criminal ransomware actors and virtual currency exchanges that launder the proceeds of ransomware. Treasury's actions today advance the Biden Administration's counter-ransomware efforts to disrupt ransomware infrastructure and actors and address abuse of the virtual currency ecosystem to launder ransom payments.

"Ransomware groups and criminal organizations have targeted American businesses and public institutions of all sizes and across sectors, seeking to undermine the backbone of our economy," said Deputy Secretary of the Treasury Wally Adeyemo. "We will continue to bring to bear all of the authorities at Treasury's disposal to disrupt, deter, and prevent future threats to the economy of the United States. This is a top priority for the Biden Administration."

Ransomware incidents have disrupted critical services and businesses globally, as well as schools, government offices, hospitals and emergency services, transportation, energy, and food companies. Reported ransomware payments in the United States so far have reached $590 million in the first half of 2021, compared to a total of $416 million in 2020. The perpetrators behind these ransomware incidents seek to harm the United States and extort the American people and our allies. Those who provide financial services to, or facilitate money laundering for, ransomware actors enable this illegal activity.

While most virtual currency activity is licit, virtual currency remains the primary mechanism for ransomware payments, and certain unscrupulous virtual currency exchanges are an

important piece of the ransomware ecosystem. The United States urges the international community to effectively implement international standards on anti-money laundering/countering the financing of terrorism (AML/CFT) in the virtual currency area, particularly regarding virtual currency exchanges.

Today's coordinated action with several U.S. government and foreign partners demonstrates how Treasury's international partnerships enhance the ability to detect and disrupt, across continents and technologies, the illicit financial activities of those who seek to harm people's livelihoods, savings, and futures for private gain.

DESIGNATION OF A VIRTUAL CURRENCY EXCHANGE AND NETWORK FOR COMPLICIT FINANCIAL SERVICES

Today's actions include the designation of **Chatex**, a virtual currency exchange, and its associated support network, for facilitating financial transactions for ransomware actors. Chatex, which claims to have a presence in multiple countries, has facilitated transactions for multiple ransomware variants. Analysis of Chatex's known transactions indicate that over half are directly traced to illicit or high-risk activities such as darknet markets, high-risk exchanges, and ransomware. Chatex has direct ties with SUEX OTC, S.R.O. (Suex), using Suex's function as a nested exchange to conduct transactions. Suex was sanctioned on September 21, 2021, for facilitating financial transactions for ransomware actors. Chatex is being designated pursuant to Executive Order (E.O.) 13694, as amended, for providing material support to Suex and the threat posed by criminal ransomware actors.

Additionally, OFAC is designating **IZIBITS OU**, **Chatextech SIA**, and **Hightrade Finance Ltd** for providing material support and assistance to Chatex, pursuant to E.O. 13694, as amended. These three companies set up infrastructure for Chatex, enabling Chatex operations.

Complementing this action, the Department of State announced 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 ransomware variant transnational organized crime group (22 U.S.C. §2708(b)(6)). The Department of State also announced a reward offer of 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.

Following an inspection by Latvia's State Revenue Service, Latvian government authorities have suspended with immediate effect the operations of Chatextech; assessed a fine for breaches of company registration and business conduct laws and regulations; and will identify current and former Chatextech board members, all non-Latvian nationals, in Latvia's registry of high-risk individuals. In addition, the Estonian Financial Intelligence Unit has revoked the license of Izibits OU after working with the United States to identify the activities of entities being designated today.

Unprincipled virtual currency exchanges like Chatex are critical to the profitability of ransomware activities, especially by laundering and cashing out the proceeds for criminals. Treasury will continue to use all available authorities to disrupt malicious cyber actors, block ill-gotten criminal proceeds, and deter additional actions against the American people. Treasury benefitted immensely from close coordination with our partners across Latvian and Estonian government agencies, including their information sharing and swift action.

DESIGNATION OF TWO RANSOMWARE OPERATORS

OFAC is designating Ukrainian **Yaroslav Vasinskyi** (Vasinskyi) and Russian **Yevgeniy Polyanin** (Polyanin) for their part in perpetuating Sodinokibi/REvil ransomware incidents against the United States. Vasinskyi deployed ransomware against at least nine U.S. companies. Vasinskyi is also responsible for the July 2021 ransomware activity against Kaseya, which caused significant disruptions to the computer networks of Kaseya's customer base. Polyanin also deployed ransomware, targeting several U.S. government entities and private-sector companies. These two individuals are part of a cybercriminal group that has engaged in ransomware activities and received more than $200 million in ransom payments paid in Bitcoin and Monero. OFAC is also designating a company owned by Polyanin, pursuant to E.O. 13694 as amended. Malicious cyber activities against the U.S. government and private sector will be aggressively investigated and pursued. Companies are encouraged to report all ransomware incidents to law enforcement, as well as any payments with a potential sanctions nexus to OFAC, and strengthen their cyber defense posture.

SANCTIONS IMPLICATIONS

As a result of today's designation, all property and interests in property of the designated targets 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 percent 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 does not implicate a sanctions nexus to any particular Ransomware-as-a-Service (RaaS) or variant.

FINCEN RELEASES UPDATED ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS

In addition, the Financial Crimes Enforcement Network (FinCEN) is releasing an update today to its 2020 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments. The updated Advisory reflects information released by FinCEN in its Financial Trend Analysis Report discussing ransomware trends, issued on October 15, 2021, and includes information on current trends and typologies of ransomware and associated payments as well as recent examples of ransomware incidents. The updated Advisory also sets out financial red flag indicators of ransomware-related illicit activity to assist financial institutions, including virtual currency service providers, in identifying and reporting suspicious transactions associated with ransomware payments, consistent with their obligations under the Bank Secrecy Act.

Click here to view identifying information on the individuals and entities designated today.

Click here to view FinCEN's Updated Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments.

FOR MORE INFORMATION ON RANSOMWARE

Please visit StopRansomware.gov, a one-stop resource for individuals and organizations of all sizes to reduce their risk of ransomware incidents 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.

###