U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats

May 6, 2022

Additional Lazarus Group Virtual Wallet Addresses Identified

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Blender.io (Blender), which is used by the Democratic People's Republic of Korea (DPRK) to support its malicious cyber activities and money-laundering of stolen virtual currency. On March 23, 2022, Lazarus Group, a DPRK state-sponsored cyber hacking group, carried out the largest virtual currency heist to date, worth almost $620 million, from a blockchain project linked to the online game Axie Infinity; Blender was used in processing over $20.5 million of the illicit proceeds. Under the pressure of robust U.S. and UN sanctions, the DPRK has resorted to illicit activities, including cyber-enabled heists from cryptocurrency exchanges and financial institutions, to generate revenue for its unlawful weapons of mass destruction (WMD) and ballistic missile programs.

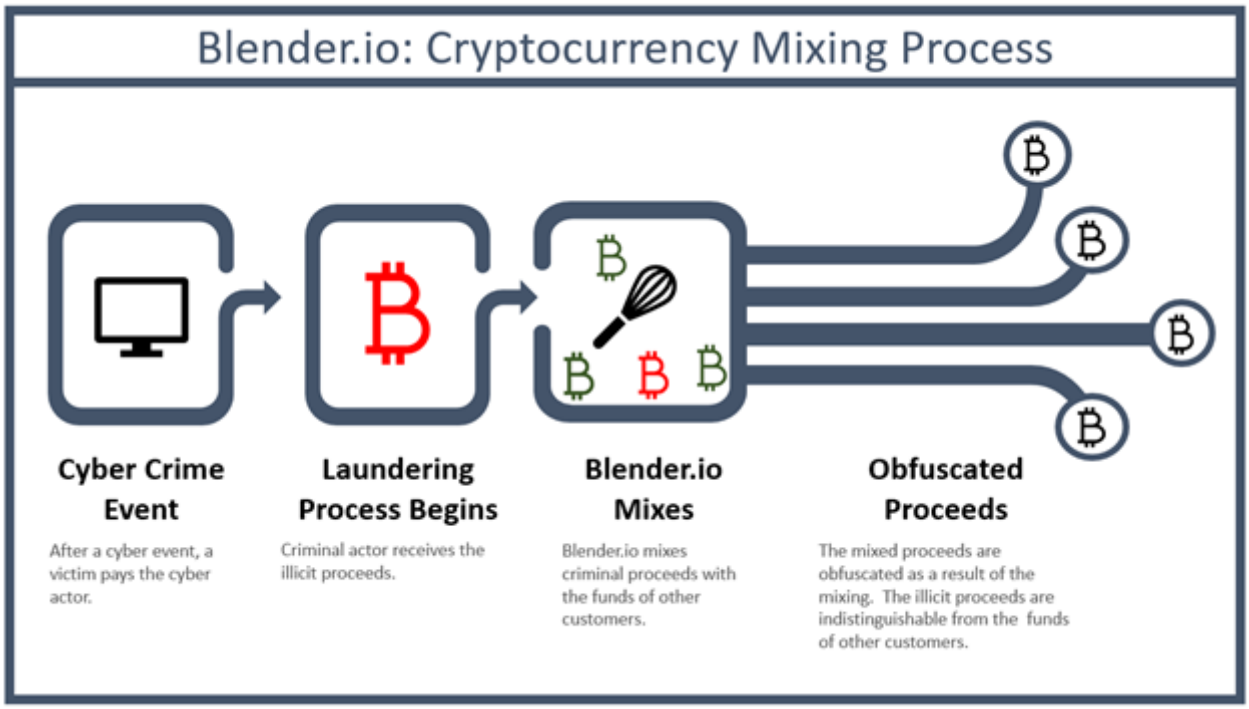
"Today, for the first time ever, Treasury is sanctioning a virtual currency mixer," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Virtual currency mixers that assist illicit transactions pose a threat to U.S. national security interests. We are taking action against illicit financial activity by the DPRK and will not allow state-sponsored thievery and its money-laundering enablers to go unanswered."

Treasury is also updating the List of Specially Designated Nationals and Blocked Persons (SDN List) to identify additional virtual currency addresses used by the Lazarus Group to launder illicit proceeds. Treasury is committed to exposing components of the virtual currency ecosystem, like Blender, that are critical to the obfuscation of the trail of stolen proceeds from illicit cyber activity. OFAC sanctioned the Lazarus Group on September 13, 2019, pursuant to Executive Order (E.O.) 13722, and identified it as an agency, instrumentality, or controlled entity of the Government of the DPRK, based on its relationship to the U.S.- and UN-designated Reconnaissance General Bureau, the DPRK's premiere intelligence organization, which is also involved in conventional arms trade.

TREASURY DESIGNATES FIRST MIXER

Blender.io (Blender) is a virtual currency mixer that operates on the Bitcoin blockchain and indiscriminately facilitates illicit transactions by obfuscating their origin, destination, and counterparties. Blender receives a variety of transactions and mixes them together before transmitting them to their ultimate destinations. While the purported purpose is to increase privacy, mixers like Blender are commonly used by illicit actors. Blender has helped transfer more than $500 million worth of Bitcoin since its creation in 2017. Blender was used in the laundering process for DPRK's Axie Infinity heist, processing over $20.5 million in illicit proceeds.

OFAC's investigation also identified Blender's facilitation of money-laundering for, among others, Russian-linked malign ransomware groups including Trickbot, Conti, Ryuk, Sodinokibi, and Gandcrab.



Blender is being designated pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign

policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

While most virtual currency activity is licit, it can be used for illicit activity, including sanctions evasion, through mixers, peer-to-peer exchangers, darknet markets, and exchanges. This includes the facilitation of heists, ransomware schemes, and other cybercrimes. Treasury continues 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 illicit payments and cyber-attacks. Those in the virtual currency industry play a critical role in implementing appropriate Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) and sanctions controls to prevent sanctioned persons and other illicit actors from exploiting virtual currency to undermine U.S foreign policy and national security interests.

The virtual currency mixers that assist criminals are a threat to U.S. national security interests. Treasury will continue to investigate the use of mixers for illicit purposes and consider the range of authorities Treasury has to respond to illicit financing risks in the virtual currency ecosystem. For example, in 2020, Treasury's Financial Crime Enforcement Network (FinCEN) assessed a $60 million civil money penalty against the owner and operator of a virtual currency mixer for violations of the Bank Secrecy Act (BSA) and its implementing regulations. Criminals have increased use of anonymity-enhancing technologies, including mixers, to help hide the movement or origin of funds. Additional information on illicit financing risks associated with mixers and other anonymity-enhancing technologies in the virtual asset ecosystem can be found in the 2022 National Money Laundering Risk Assessment.

ADDITIONAL LAZARUS GROUP WALLET

OFAC is identifying four additional virtual currency wallet addresses used by the Lazarus Group to launder the remainder of stolen proceeds from the March 2022 Axie Infinity heist. This builds upon OFAC's April 14, 2022, attribution of DPRK's Lazarus Group as the perpetrators of the Axie Infinity heist and identification of the original getaway wallet address. Treasury is committed to tracing illicit virtual currency and blocking associated wallets and addresses wherever found.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the entity above, Blender.io, that is in the United States or in the possession or control of U.S. persons is blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

For identifying information on the entity sanctioned today, click here.

For the U.S. government's 2020 DPRK Cyber Threat Advisory, click here.

For information on complying with virtual currency sanctions, see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry here.

###