U.S. DEPARTMENT OF THE TREASURY

Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash

August 23, 2023

Concurrent Treasury sanctions and DOJ indictments hold to account founders of mixing service that laundered stolen virtual assets for North Korea

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Roman Semenov, one of three co-founders of the sanctioned virtual currency mixer Tornado Cash, for his role in providing material support to Tornado Cash and to the Lazarus Group, a state-sponsored hacking group that is an instrumentality of the Democratic People's Republic of Korea (DPRK or North Korea). Tornado Cash has been used to launder funds for criminal actors since its creation in 2019, including to obfuscate hundreds of millions of dollars in virtual currency stolen by Lazarus Group hackers.

This sanctions designation was conducted in coordination with the U.S. Department of Justice (DOJ), which unsealed an indictment against Semenov and a second co-founder of Tornado Cash, Roman Storm, who was arrested today by the Federal Bureau of Investigation and the Internal Revenue Service, Criminal Investigation. The DOJ charged Semenov and Storm with conspiracy to commit money laundering, conspiracy to operate an unlicensed money transmitting business, and conspiracy to commit sanctions violations. A third co-founder of Tornado Cash, Alexey Pertsev, was arrested on related money laundering charges in the Netherlands in August 2022 by Dutch law enforcement authorities.

The Lazarus Group, which was sanctioned by the United States in 2019, used Tornado Cash to obfuscate the movement of over $455 million stolen in the March 2022 attack on Axie Infinity's Ronin network bridge, the largest known virtual currency heist to date. The Lazarus Group subsequently used Tornado Cash to launder more than $96 million of funds derived from the June 24, 2022 cyber-enabled heist on Harmony's Horizon bridge, and at least $7.8 million from the August 2, 2022 Nomad heist. This revenue provides the DPRK with resources that it uses to support its unlawful ballistic missile and nuclear weapons programs.

"Even after they knew the Lazarus Group was laundering hundreds of millions of dollars' worth of stolen virtual currency through their mixing service for the benefit of the Kim regime, Tornado

Cash's founders continued to develop and promote the service and did not take meaningful steps to reduce its use for illicit purposes," said Deputy Secretary of the Treasury Wally Adeyemo. "Today's actions by IRS Criminal Investigators and OFAC demonstrate Treasury's commitment to continue going after those who recklessly operate and support dangerous virtual currency mixing services that threaten our national security."

Today's designation and indictments build on earlier actions to expose elements of the virtual currency ecosystem that cybercriminals, including the Lazarus Group, use to obfuscate the origins and destinations of proceeds from their illicit activities. It also underscores Treasury's commitment to protecting the integrity of our financial system, including the virtual currency ecosystem, and to disrupt the ability of the DPRK regime to raise funds through illicit activity.

In 2022, OFAC sanctioned Tornado Cash and Blender.io, which both provided mixing services to the Lazarus Group. This year, OFAC sanctioned two over-the-counter virtual currency traders who facilitated the conversion of stolen virtual currency to fiat currency for DPRK actors working with the Lazarus Group. Tomorrow, Treasury's Financial Crimes Enforcement Network (FinCEN) will host a FinCEN Exchange focused on countering the DPRK's abuse of the digital ecosystem, which will include representatives from Treasury, law enforcement, and the financial sector. Treasury will continue to utilize all of its tools to counter the DPRK's cyber-enabled illicit finance threats.

ROMAN SEMENOV: A KEY DEVELOPER OF TORNADO CASH

Roman Semenov (**Semenov**), a citizen of Russia, co-founded Tornado Cash as a mixing service to increase the anonymity of users' transactions. Semenov was actively involved in promoting Tornado Cash in media and on online platforms, where he provided Tornado Cash users with advice to anonymize their transactions. After Semenov was alerted that Tornado Cash was being used to launder large volumes of stolen virtual currency for the Lazarus Group, he and his fellow co-founders continued to pay for infrastructure supporting the Tornado Cash service and took steps to increase the anonymity of the Tornado Cash service without appropriate measures to address the known illicit use by the DPRK.

In April 2022, Semenov learned that an Ethereum address that was publicly attributed to the Lazarus Group and identified on the Specially Designated Nationals and Blocked Persons List (SDN List), containing hundreds of millions of dollars in stolen proceeds from the widely publicized $620 million Ronin bridge heist, was being used to send funds through Tornado Cash's service. Semenov and his fellow co-founders put in place a front-end sanctions screening service, but did so knowing that this would be easy to evade, and did not take steps to sufficiently address active abuse by the DPRK. Despite his possession of information from publicly available blockchain analysis and

inquiries from media, Semenov consistently ignored or downplayed the evidence that Tornado Cash was being used to launder stolen virtual currency for the DPRK, continued to participate in the operation and maintenance of the Tornado Cash service, and took no meaningful actions to prevent or mitigate the risk of actors using Tornado Cash to launder proceeds from their illicit activities following subsequent high profile heists.

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 North Korea. The Lazarus Group has operated for more than 10 years and is believed to have stolen over $2 billion worth of digital assets across multiple thefts. Due to the pressure of robust U.S. and United Nations sanctions, the DPRK has resorted to using illicit tactics, such as cyber-enabled heists perpetrated by the Lazarus Group, to generate revenue for its unlawful weapons of mass destruction and ballistic missile programs.

Semenov is being designated pursuant to E.O. 13694, as amended by E.O. 13757, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsections (a)(ii) or (a)(iii)(A) of E.O. 13694, as amended, or any person whose property and interests in property are blocked pursuant to E.O. 13694, as amended; and pursuant to E.O. 13722 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of North Korea, a person whose property and interests in property are blocked pursuant to E.O. 13722.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated individual that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC's regulations generally prohibit all dealings by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of blocked or designated persons.

In addition, persons that engage in certain transactions with the individual designated today may themselves be exposed to designation.

The power and integrity of sanctions derive not only from OFAC's ability to designate and add persons to the SDN List but also from OFAC's willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an

OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please refer to OFAC's website.

For more information on the individual designated today, click here.

###