U.S. DEPARTMENT OF THE TREASURY

Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs

April 24, 2023

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned three individuals for providing support to the Democratic People's Republic of Korea (DPRK) through illicit financing and malicious cyber activity. The DPRK launders stolen virtual currency and deploys information technology (IT) workers to fraudulently obtain employment to generate revenue in virtual currency to support the regime and its unlawful weapons of mass destruction and ballistic missile programs. Today's actions have been taken in close coordination with the Republic of Korea.

"The DPRK's use of illicit facilitation networks to access the international financial system and generate revenue using virtual currency for the regime's unlawful weapons of mass destruction(WMD) and ballistic missile programs directly threatens international security," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "The United States and our partners are committed to safeguarding the international financial system and preventing its use in the DPRK's destabilizing activities, especially in light of the DPRK's three launches of intercontinental ballistic missiles (ICBMs) this year alone."

SUPPORT TO DPRK MALICIOUS CYBER ACTIVITY

Wu Huihui (Wu) is being designated pursuant to Executive Order (E.O.) 13722 for providing material support to the Lazarus Group, which was previously designated pursuant to that same authority on September 13, 2019. **Cheng Hung Man** (Cheng) is being designated pursuant to E.O. 13722 for providing material support to Wu.

The Lazarus Group targets institutions such as financial, manufacturing, publishing, media, entertainment, and international shipping companies, as well as government and military and critical infrastructure, using tactics such as cyber espionage, data theft, monetary heists, and destructive malware operations. The group is controlled by the Reconnaissance General Bureau (RGB), the DPRK's primary intelligence bureau and main entity responsible for the country's malicious cyber activities, and is involved in the trade of DPRK arms. On March 23, 2022, the

Lazarus Group carried out the largest virtual currency heist to date, stealing almost $620 million in virtual currency from a blockchain project linked to the online game Axie Infinity.

Since at least late 2017, the DPRK has been engaged in virtual currency thefts and fraud schemes to generate revenue for its unlawful ballistic missile and weapons of mass destruction programs. According to public reporting, DPRK cyber actors were able to steal an estimated $1.7 billion worth of virtual currency through various hacks in 2022 alone. The DPRK often launders the stolen virtual currency through a complicated process to convert stolen virtual currency into fiat currency. The DPRK leverages a network of over-the-counter (OTC) virtual currency traders to convert crypto currency into fiat currency. Frequently, DPRK actors use these networks of OTC traders, including People's Republic of China (PRC)-based OTC traders, to conduct transactions on their behalf to avoid detection by financial institutions or competent authorities.

Wu is a PRC-based OTC virtual currency trader who facilitated the conversion of virtual currency stolen by DPRK actors working with the Lazarus Group to fiat currency. In 2021, **Wu** processed multiple transactions that converted millions of dollars' worth of virtual currency into fiat currency for DPRK cyber actors. **Cheng** is a Hong Kong-based OTC trader who worked with **Wu** to remit payment to companies in exchange for virtual currency. Cheng utilized front companies to enable DPRK actors to bypass countering illicit finance requirements at financial institutions and access the U.S. financial system. **Cheng** worked with **Wu** and other virtual currency OTC traders who facilitate conversion of virtual currency stolen by DPRK hackers into fiat currency for use by the DPRK government.

ILLICIT ACCESS TO THE INTERNATIONAL FINANCIAL SYSTEM

OFAC is also designating **Sim Hyon Sop** (Sim) pursuant to E.O. 13382, for acting for or on behalf of the Korea Kwangson Banking Corp (KKBC), an entity previously designated under E.O. 13382, an authority that targets proliferators of WMD and their supporters. KKBC was designated for providing financial services in support of both Tanchon Commercial Bank and Korea Hyoksin Trading Corporation, entities previously designated pursuant to E.O. 13382.

Sim is a KKBC Deputy Representative who recently relocated to Dandong, China. The DPRK's Foreign Trade Bank, also previously designated under E.O. 13382, is KKBC's parent company. According to the Financial Crimes Enforcement Network (FinCEN), the DPRK uses and maintains a network of financial representatives, primarily in the PRC, who operate as agents for DPRK

financial institutions. In this capacity, these representatives orchestrate schemes, set up shell companies, and manage surreptitious bank accounts to move and disguise illicit funds and finance the DPRK's WMD and ballistic missile programs. In his position with KKBC, **Sim** has coordinated millions of dollars in financial transfers for the DPRK.

The DPRK also generates revenue through the deployment of IT workers who fraudulently obtain employment in the technology and virtual currency industries. The DPRK maintains a workforce of thousands of highly skilled IT workers around the world to generate revenue that contributes to its unlawful WMD and ballistic missile programs. Since September 2021, Sim has received tens of millions of dollars in virtual currency. That virtual currency was, in part, derived from DPRK individuals unknowingly hired by U.S.-based companies to provide IT development work. These DPRK IT workers typically use fake personas to apply for jobs at these companies. When the IT workers obtain employment, they are known to request to be paid in virtual currency and send the majority of their salaries through a complicated laundering pattern to funnel these illegally obtained funds back to the DPRK. **Sim** appears to be receiving money from IT development work being fraudulently conducted by DPRK individuals abroad and, separately, directing OTC traders, including **Wu** and **Cheng**, to send payments to front companies with funds derived from stolen virtual currency, so that those front companies can make payments in fiat currency for goods, such as tobacco and communications devices, on behalf of the DPRK regime.

Today's action is the result of OFAC's ongoing collaboration with the Department of Justice and the Federal Bureau of Investigation. On April 18, 2023, a federal indictment was returned in the U.S District Court for the District of Columbia for **Wu**, **Cheng**, and **Sim**. Today's action was also closely coordinated with the Republic of Korea, which is also designating Sim for his illicit activities

SANCTIONS IMPLICATIONS

As a result of today's action, pursuant to E.O. 13722 and E.O. 13382, all property and interests in property of the persons named above that are in the United States, or in the possession or control of U.S. persons, are 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.

In addition, persons that engage in certain transactions with the individuals or entities designated today may themselves be exposed to designation. Furthermore, any foreign

financial institution that knowingly facilitates a significant transaction or provides significant financial services for any of the individuals or entities designated today could be subject to U.S. correspondent or payable-through account sanctions.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List, but also from its 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 additional information regarding the DPRK's IT workers, see the May 16, 2022, Guidance on the Democratic People's Republic of Korea Information Technology Workers.

For detailed information on the process to submit a request for removal from an OFAC sanctions list.

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

Find identifying information on the individuals sanctioned today here.

###