Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group

March 2, 2020

WASHINGTON – The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) today sanctioned two Chinese nationals involved in laundering stolen cryptocurrency from a 2018 cyber intrusion against a cryptocurrency exchange. This cyber intrusion is linked to Lazarus Group, a U.S.-designated North Korean state-sponsored malicious cyber group. Specifically, OFAC is designating 田寅寅, Tian Yinyin (Tian), and 李家东, Li Jiadong (Li), for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a malicious cyber-enabled activity. Tian and Li are also being designated for having materially assisted, sponsored or provided financial, material, or technological support for, or goods or services to or in support of, Lazarus Group.

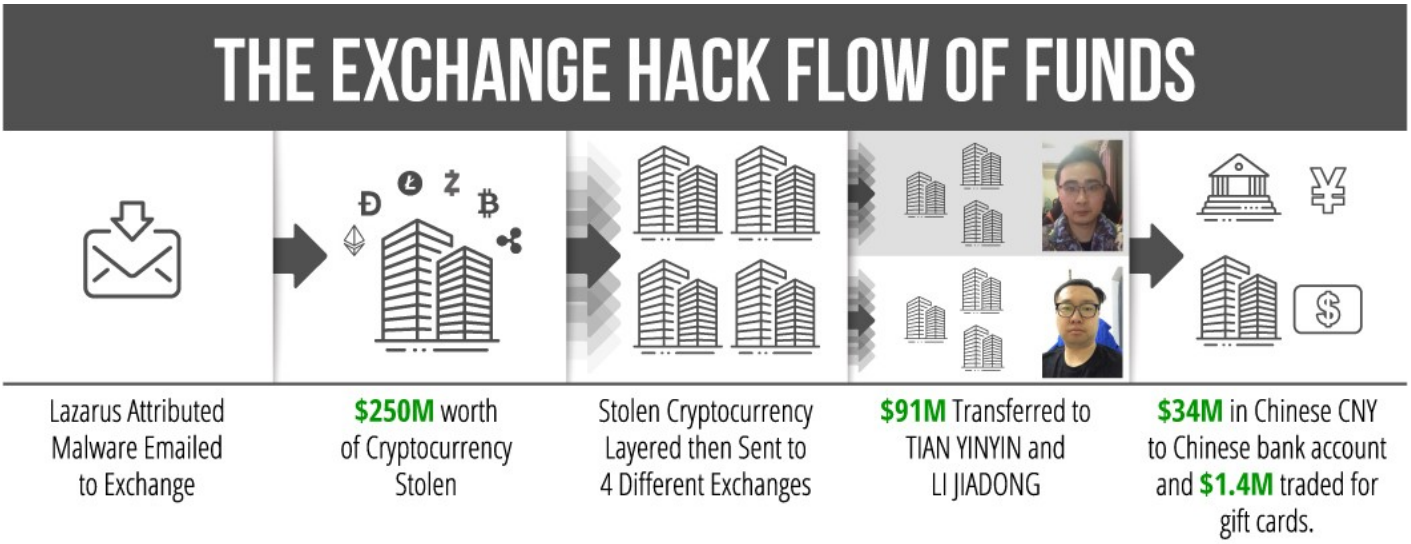
"The North Korean regime has continued its widespread campaign of extensive cyber-attacks on financial institutions to steal funds," said Secretary Steven T. Mnuchin. "The United States will continue to protect the global financial system by holding accountable those who help North Korea engage in cyber-crime."

Tian and Li's Activities

The Democratic People's Republic of Korea (DPRK) trains cyber actors to target and launder stolen funds from financial institutions. Tian and Li received from DPRK-controlled accounts approximately $91 million stolen in an April 2018 hack of a cryptocurrency exchange (referred to hereinafter as "the exchange"), as well as an additional $9.5 million from a hack of another exchange. Tian and Li transferred the currency among addresses they held, obfuscating the origin of the funds.

In April 2018, an employee of the exchange unwittingly downloaded DPRK-attributed malware through an email, which gave malicious cyber actors remote access to the exchange and unauthorized access to customers' personal information, such as private keys used to access virtual currency wallets stored on the exchange's servers. Lazarus Group cyber actors used the private keys to steal virtual currencies ($250 million dollar equivalent at date of theft) from this exchange, accounting for nearly half of the DPRK's estimated virtual currency heists that year.

Tian ultimately moved the equivalent of more than $34 million of these illicit funds through a newly added bank account linked to his exchange account. Tian also transferred nearly $1.4 million dollars' worth of Bitcoin into prepaid Apple iTunes gift cards, which at certain exchanges can be used for the purchase of additional Bitcoin.



Tian and Li are being designated pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757. Additionally, they are being designated pursuant to E.O. 13722.

OFAC closely coordinated today's action with the U.S. Attorney's Office for the District of Columbia and the Internal Revenue Service's Criminal Investigation Division. Treasury supports the concurrent law enforcement-related actions taken against these and additional individuals and accounts.

As a result of today's action, all property and interests in property of these individuals 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 individuals 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 designated today could be subject to U.S. correspondent account or payable-through sanctions.

North Korea's History of Malicious Cyber-Enabled Activities

On September 13, 2019, Treasury identified North Korean hacking groups commonly known within global cyber security private industry as “Lazarus Group,” “Bluenoroff,” and “Andariel” as agencies, instrumentalities, or controlled entities of the Government of North Korea, pursuant to E.O. 13722, based on their relationship to the Reconnaissance General Bureau (RGB), North Korea’s primary intelligence agency. Lazarus Group, Bluenoroff, and Andariel are controlled by the U.S.- and United Nations (UN)-designated RGB.

North Korea’s malicious cyber activity is a key revenue generator for the regime, from the theft of fiat currency at conventional financial institutions to cyber intrusions targeting cryptocurrency exchanges. The August 2019 UN Security Council 1718 Committee Panel of Experts report estimates that North Korea had attempted to steal as much as $2 billion, of which $571 million is attributed to cryptocurrency theft. This revenue allows the North Korean regime to continue to invest in its illicit ballistic missile and nuclear programs.

Given the illicit finance risk that cryptocurrency and other digital assets pose, in June 2019 the Financial Action Task Force (FATF) amended its standards to require all countries to regulate and supervise such service providers, including exchangers, and to mitigate against such risks when engaging in cryptocurrency transactions. Virtual asset service providers and traditional institutions should remain vigilant and alert to substantial changes in customers’ activities, as their business may be used to facilitate the transfer of stolen proceeds. The United States is particularly concerned about platforms that provide anonymous payment and storage functionality without transaction monitoring, suspicious activity reporting, or customer due diligence, among other obligations.

DPRK cyber actors actively target the cryptocurrency community and are known to employ a variety of fake cryptocurrency trading programs that contain malware. In April 2018, the Lazarus Group leveraged previously used malware code from the now defunct cryptocurrency application Celas Trade Pro — software both developed and offered by the Lazarus Group registered website called Celas Limited. Creating illegitimate websites and malicious software to conduct phishing attacks against the virtual currency sector is a pattern previously seen from North Korean cyber criminals.

DPRK malicious cyber proceeds are often transferred to cryptocurrency exchanges and peer-to-peer marketplaces with negligible customer screening compliance programs, or individual peer-to-peer or over-the-counter traders operating on exchanges that do not screen their customers. Stolen cryptocurrency may be layered using various schemes, traded for fiat currency,

deposited in bank accounts, and traded for gift cards. Proceeds from DPRK malicious cyber activities often end up at Chinese financial institutions.

Delisting of Two Russian Entities

In addition to today's designation, OFAC is delisting two Russian entities, Independent Petroleum Company (IPC) and its subsidiary AO NNK-Primornefteproduct (NNK-P). IPC was originally designated on June 1, 2017 pursuant to E.O. 13722 for operating in the transportation sector in North Korea. IPC shipped over $1 million worth of petroleum products to North Korea. Following this designation, IPC's parent company, Alliance Oil Company (AOC), ceased all export activities and instituted a global compliance program. Treasury recognizes the actions that IPC, NNK-P, and parent company AOC have taken to ensure they do not engage in activity that may benefit North Korea.

U.S. sanctions need not be permanent; sanctions are intended to bring about a positive change of behavior. The United States has made clear that the removal of sanctions is available for persons designated under North Korea-related authorities, who take concrete and meaningful actions to stop enabling North Korea's sanctions circumvention. As a result of today's delisting action, all property and interests in property that had been blocked as a result of IPC and NNK-P's respective designations are unblocked, and all otherwise lawful transactions involving U.S. persons and these two entities are no longer prohibited.

Read identifying information related to today's action here.

####