Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups

September 13, 2019

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity on critical infrastructure. Today's actions identify North Korean hacking groups commonly known within the 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 Executive Order (E.O.) 13722, based on their relationship to the Reconnaissance General Bureau (RGB). Lazarus Group, Bluenoroff, and Andariel are controlled by the U.S.- and United Nations (UN)-designated RGB, which is North Korea's primary intelligence bureau.

"Treasury is taking action against North Korean hacking groups that have been perpetrating cyber attacks to support illicit weapon and missile programs," said Sigal Mandelker, Treasury Under Secretary for Terrorism and Financial Intelligence. "We will continue to enforce existing U.S. and UN sanctions against North Korea and work with the international community to improve cybersecurity of financial networks."

MALICIOUS CYBER ACTIVITY BY LAZARUS GROUP, BLUENOROFF, AND ANDARIEL

Lazarus Group targets institutions such as government, military, financial, manufacturing, publishing, media, entertainment, and international shipping companies, as well as critical infrastructure, using tactics such as cyber espionage, data theft, monetary heists, and destructive malware operations. Created by the North Korean Government as early as 2007, this malicious cyber group is subordinate to the 110th Research Center, 3rd Bureau of the RGB. The 3rd Bureau is also known as the 3rd Technical Surveillance Bureau and is responsible for North Korea's cyber operations. In addition to the RGB's role as the main entity responsible for North Korea's malicious cyber activities, the RGB is also the principal North Korean intelligence agency and is involved in the trade of North Korean arms. The RGB was designated by OFAC on January

2, 2015 pursuant to E.O. 13687 for being a controlled entity of the Government of North Korea. The RGB was also listed in the annex to E.O. 13551 on August 30, 2010. The UN also designated the RGB on March 2, 2016.

Lazarus Group was involved in the destructive WannaCry 2.0 ransomware attack which the United States, Australia, Canada, New Zealand and the United Kingdom publicly attributed to North Korea in December 2017. Denmark and Japan issued supporting statements and several U.S. companies took independent actions to disrupt the North Korean cyber activity. WannaCry affected at least 150 countries around the world and shut down approximately three hundred thousand computers. Among the publicly identified victims was the United Kingdom's (UK) National Health Service (NHS). Approximately one third of the UK's secondary care hospitals — hospitals that provide intensive care units and other emergency services — and eight percent of general medical practices in the UK were crippled by the ransomware attack, leading to the cancellation of more than 19,000 appointments and ultimately costing the NHS over $112 million, making it the biggest known ransomware outbreak in history. Lazarus Group was also directly responsible for the well-known 2014 cyber-attacks of Sony Pictures Entertainment (SPE).

Also designated today are two sub-groups of Lazarus Group, the first of which is referred to as Bluenoroff by many private security firms. Bluenoroff was formed by the North Korean government to earn revenue illicitly in response to increased global sanctions. Bluenoroff conducts malicious cyber activity in the form of cyber-enabled heists against foreign financial institutions on behalf of the North Korean regime to generate revenue, in part, for its growing nuclear weapons and ballistic missile programs. Cybersecurity firms first noticed this group as early as 2014, when North Korea's cyber efforts began to focus on financial gain in addition to obtaining military information, destabilizing networks, or intimidating adversaries. According to industry and press reporting, by 2018, Bluenoroff had attempted to steal over $1.1 billion dollars from financial institutions and, according to press reports, had successfully carried out such operations against banks in Bangladesh, India, Mexico, Pakistan, Philippines, South Korea, Taiwan, Turkey, Chile, and Vietnam.

According to cyber security firms, typically through phishing and backdoor intrusions, Bluenoroff conducted successful operations targeting more than 16 organizations across 11 countries, including the SWIFT messaging system, financial institutions, and cryptocurrency exchanges. In one of Bluenoroff's most notorious cyber activities, the hacking group worked jointly with Lazarus Group to steal approximately $80 million dollars from the Central Bank of

Bangladesh's New York Federal Reserve account. By leveraging malware similar to that seen in the SPE cyber attack, Bluenoroff and Lazarus Group made over 36 large fund transfer requests using stolen SWIFT credentials in an attempt to steal a total of $851 million before a typographical error alerted personnel to prevent the additional funds from being stolen.

The second Lazarus Group sub-group designated today is Andariel. It focuses on conducting malicious cyber operations on foreign businesses, government agencies, financial services infrastructure, private corporations, and businesses, as well as the defense industry. Cybersecurity firms first noticed Andariel around 2015, and reported that Andariel consistently executes cybercrime to generate revenue and targets South Korea's government and infrastructure in order to collect information and to create disorder.

Specifically, Andariel was observed by cyber security firms attempting to steal bank card information by hacking into ATMs to withdraw cash or steal customer information to later sell on the black market. Andariel is also responsible for developing and creating unique malware to hack into online poker and gambling sites to steal cash.

According to industry and press reporting, beyond its criminal efforts, Andariel continues to conduct malicious cyber activity against South Korea government personnel and the South Korean military in an effort to gather intelligence. One case spotted in September 2016 was a cyber intrusion into the personal computer of the South Korean Defense Minister in office at that time and the Defense Ministry's intranet in order to extract military operations intelligence.

In addition to malicious cyber activities on conventional financial institutions, foreign governments, major companies, and infrastructure, North Korea's cyber operations also target Virtual Asset Providers and cryptocurrency exchanges to possibly assist in obfuscating revenue streams and cyber-enabled thefts that also potentially fund North Korea's WMD and ballistic missile programs. According to industry and press reporting, these three state-sponsored hacking groups likely stole around $571 million in cryptocurrency alone, from five exchanges in Asia between January 2017 and September 2018.

U.S. GOVERNMENT EFFORTS TO COMBAT NORTH KOREAN CYBER THREATS

Separately, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Cyber Command (USCYBERCOM) have in recent months worked in tandem to disclose malware samples to the private cybersecurity industry, several of which were later attributed to North Korean cyber actors, as part of an ongoing effort to protect the

U.S. financial system and other critical infrastructure as well as to have the greatest impact on improving global security. This, along with today's OFAC action, is an example of a government-wide approach to defending and protecting against an increasing North Korean cyber threat and is one more step in the persistent engagement vision set forth by USCYBERCOM.

As a result of today's action, all property and interests in property of these entities, and of any entities that are owned, directly or indirectly, 50 percent or more by the designated entities, that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. OFAC's regulations generally prohibit all dealings by U.S. persons or within (or 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 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 entities designated today could be subject to U.S. correspondent account or payable-through sanctions.

Information on the entities designated today.