Cyber Attacks on Commercial Banks Possibly Linked to North Korea

An investigation recently opened by federal authorities – the FBI and U.S. Attorney’s Office in Los Angeles - and analyses by private cybersecurity firms such as Symantec and Bae Systems in the past month have renewed suspicions of potential new North Korean cyberattacks that raises concerns on the rapid development of the rogue state’s cyber capability. The alleged attacks this time are linked to a recent string of digital heists on banks in Asia and in Ecuador in the past few months, including an attempt to steal about US$951 million from the Bangladesh Bank (BB), the Central Bank of Bangladesh’s account at the Federal Reserve Bank of New York through the SWIFT payment system in February 2016, of which US$81 million remains unaccounted for, an earlier attempt to steal US$1 million from the Tien Phong Bank in Vietnam in September 2015, unreported until this May, and a potentially unrelated attack on the Banco del Austro in Ecuador, where US$12 million was lost.

- Analysis by Symantec on the BB cyber-attack found a distinct file wiping code that exhibits the same unique characteristics from a larger toolkit that was previously used by a broad threat group known as Lazarus. This group have been linked to attacks in the U.S. and South Korea, including attacks on South Korean banks and broadcasters in 2013, and the Sony Pictures Entertainment cyber-attack in November 2014, which the FBI later concluded was the work of the North Korean government. It also found evidence that this same group had targeted a bank in the Philippines this year.

- Similar findings on the BB cyber-attack this past month by Bae Systems corroborate this indirect link to North Korea, which also found that similar tactics targeting the SWIFT payment system used in the BB attack may have been previously used on the Tien Phong Bank last September.

- The SWIFT payment system – made up of more than 11,000 financial institutions and headquartered in Belgium- sent out an alert on April 25 reassuring its customers that the malware used in the BB attack had no impact on its network or core messaging services, and that the hackers had accessed the system through local customers’ credentials and used malicious software to cover their tracks. It sent out another alert on May 13 about a second attack, later revealed to be against Tien Phong. The alert pointed out that the malware used is “part of a wider and highly adaptive campaign targeting banks.”
May 31, 2016

- If these attacks are definitively linked to North Korea it would demonstrate further advancement of the country’s cyber capabilities in the aftermath of the 2014 cyber-attack against Sony Pictures Entertainment.

- A CSIS study found that the North does not discriminate between civilian and military targets in terms of their growing cyber capabilities, and is actively trying to build an asymmetric capability in this field to complement their WMD and ballistic missile programs.

- If the money is found to have been routed to North Korea or to some third party affiliated with North Korea, this would represent a new form of cyber robbery that the regime has not engaged in the past, possibly linked to the desire for new sources of hard currency in the aftermath of tightened sanctions.