



North Korea Cyber Crime Shifts Gears

OE Watch Commentary: According to the Korea Internet and Security Agency (KISA), the number of attacks emanating from North Korea on virtual money targets in South Korea increased 3.7 times in the last year. In the past when one considered cyber attacks from North Korea, it was predominantly about disruption. Although inconclusive, it is believed that the 2014 malware attack against Sony Pictures had a North Korea connection and was a classic case of a cyber attack dedicated to disrupt a company and even an industry. Now, it appears that the Pyongyang regime has opened up another cyber warfare front, which is potentially more destabilizing globally. Now it is all about stealing cryptocurrencies and Bitcoin seems to be in North Korea's crosshairs.

Source: “북한 해커들 금융보안원 사칭해 비트코인 해킹” (North Korean Hackers Target Bitcoin as source of Financial Security for Regime),” *Coin News*, 10 November 2017, <https://blog.naver.com/eflora/221137312401>

“South Korea’s internet security authorities have pointed to a tremendous rise in malware attacks where North Korean hackers are looking for Bitcoin to fund the Kim Jong-un regime...”

According to the Korea Communications Agency, the number of malicious codes detected increased from 1,438 in 2016 to 5,366 during the same period January to September 2017.”

As the accompanying passage discusses, in 2016 there were 1,438 cases of computer crimes targeting coin-to-coin payments in South Korea, by North Korean hackers. From January to September 2017 there have been 5,366 cases of coin-to-coin malware targeting. Hundreds of millions of dollars of virtual currency has been stolen. The passage claims that this is being done to “fund the Kim Jong-un regime.”

North Korea has always struggled to finance its shaky regime. As a result it continues to extort the international community when possible. Meanwhile Pyongyang also engages in a variety of illicit activities including but not limited to the counterfeiting of US \$100 bills or “supernotes,” and drug production and smuggling across the Chinese border primarily along the Tumen River sector. All of these activities continue to be undertaken to beat the ill effects of international sanctions against the regime.

For years there has been some level of sanctions targeting North Korea for its human rights record and its constant drive to build a nuclear arsenal and the delivery systems capable of striking out against its enemies. Recent sanctions may be having an adverse effect on Pyongyang, and although China is still an ally, there hasn't been the usual unqualified support from Beijing that North Korea may have been accustomed too. As a result, economic instability is likely on the rise. Consider the wave of fishing boats washing up on Japanese shores over the last 12 months. Is this a signal of a deteriorating economic situation in North Korea?

North Korea appears as hard pressed as ever to fund its regime. Cryptocurrencies might well be considered the regime's way out. Pyongyang seems to have gone all in on stealing cryptocurrencies and South Korea seems to have borne the brunt of North Korea's attacks thus far. **End OE Watch Commentary (Billingsley)**

“According to the Korea Communications Agency, the number of malicious codes detected increased from 1,438 in 2016 to 5,366 during the same period January to September 2017.”



North Korea Flag on top of world map with code.

Source: Created by Dodge Billingsley with background from <https://pixabay.com/en/matrix-code-data-networking-1735640/>, CC0.