Alert: Cyberattack by North Korean Cyber Actors, TraderTraitor

（Provisional Translation）

The National Police Agency (NPA), the U.S. Federal Bureau of Investigation (FBI), and the U.S. Department of Defense Cyber Crime Center (DC3) are jointly alerting that North Korean cyber threat actors, TraderTraitor, stole cryptoasset worth approximately 48.2 billion yen from a cryptoasset company, DMM Bitcoin.

TraderTraitor has been identified as the cyber threat associated with cryptoasset thefts in the joint Cybersecurity Advisory issued from the FBI, U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Administration (CISA) and the U.S. Department of Treasury on April 18, 2022. This group is considered as a part of the "Lazarus Group," which is said to be a subordinate organization of the North Korean authorities. The Japanese government also issued a joint alert between the Financial Services Agency (FSA), NPA and the National center of Incident and readiness and Strategy for Cybersecurity (NISC) against Lazarus Group as "a cyber actor called as Lazarus" on October 14, 2022. Lazarus has been repeatedly identified in several alerts.

Regarding the cryptoasset theft by North Korea, the FBI released an announcement on September 3, 2024, detailing the North Korean social engineering scheme and mitigation measures for the threat.

The investigation and analysis by the National Cyber Department of the Kanto Regional Police Bureau of the NPA and the Tokyo Metropolitan Police Department reveals the North Korean specific social engineering scheme. This alert, providing examples of cyber theft tactics and mitigation measures, aims to encourage target organizations and businesses to take appropriate cyber security measures. It seems that North Korea continues to attempt to steal cryptoasset. Individuals and businesses involved in cryptoasset transactions should be aware the threat in cyberspace and immediately provide the information to the competent ministries and agencies such as FSA, the police, NISC or cyber security-related organizations if any suspicious communications are recognized on their networks.

For more detail information, visit our Japanese version website.