TechXplore

UN experts: North Korean hackers stole record virtual assets

February 8 2023, by Edith M. Lederer

In this photo provided by the North Korean government, North Korean leader Kim Jong Un delivers a speech during a feast to mark the 75th founding anniversary of the Korean People's Army at an unspecified place in North Korea Tuesday, Feb. 7, 2023. Independent journalists were not given access to cover the event depicted in this image distributed by the North Korean government. The content of this image is as provided and cannot be independently verified. Korean language watermark on image as provided by source reads: "KCNA" which is the abbreviation for Korean Central News Agency. Credit: Korean

Central News Agency/Korea News Service via AP

North Korean hackers working for the government stole record-breaking virtual assets last year estimated to be worth between $630 million and more than $1 billion, U.N. experts said in a new report.

The panel of experts said in the wide-ranging report seen Tuesday by The Associated Press that the hackers used increasingly sophisticated techniques to gain access to digital networks involved in cyberfinance, and to steal information that could be useful in North Korea's nuclear and ballistic missile programs from governments, individuals and companies.

With growing tensions on the Korean Peninsula, the report said North Korea continued to violate U.N. sanctions, producing weapons-grade nuclear material, and improving its ballistic missile program, which "continued to accelerate dramatically."

In 2022, the Democratic People's Republic of Korea—the North's official name—launched at least 73 ballistic missiles and missiles combining ballistic and guidance technologies including eight intercontinental ballistic missiles, the panel said. And 42 launches, including the test of a reportedly new type of ICBM and a new solid-fueled ICBM engine, were conducted in the last four months of the year.

North Korea's leader Kim Jong Un ordered an "exponential increase of the country's nuclear arsenal" in January, and the panel said "a new law discussed an increased focus on tactical nuclear capability, a new first-use doctrine, and the 'irreversible nature' of the DPRK's nuclear status."

"The ability to carry out an unexpected nuclear strike on any regional or international target, described in DPRK's new law on nuclear doctrine and progressively in public statements since 2021, is consistent with the observed production, testing, and deployment of its tactical and strategic delivery systems," the experts said in the report to the U.N. Security Council.

The panel said that South Korean authorities quoted in media reports "estimated that state sponsored DPRK cyber threat actors had stolen virtual assets worth around $1.2 billion globally since 2017, including about $630 million in 2022 alone."

The experts monitoring sanctions against North Korea said an unnamed cybersecurity firm "assessed that in 2022, DPRK cybercrime yielded cyber currencies worth over $1 billion at the time of the threat, which is more than double the total proceeds in 2021."

The variation in the U.S. dollar value of cryptocurrency in recent months is likely to have affected these estimates, the panel said, "but both show that 2022 was a record-breaking year for DPRK virtual asset theft."

The panel said three groups that are part of the Reconnaissance General Bureau, North Korea's primary foreign intelligence organization, "continued illicitly to target victims to generate revenue and solicit information of value to the DPRK including its weapons programs"—Kimsuky, Lazarus Group and Andariel.

Between February and July 2022, the panel said, the Lazarus Group "reportedly targeted energy providers in multiple member states using a vulnerability" to install malware and gain long-term access. It said this "aligns with historical Lazarus intrusions targeting critical infrastructure and energy companies … to siphon off proprietary intellectual property."

Lazarus Group's primary focus is on specific types of industry, aerospace and defense and conventional finance and cryptocurrencies, with the objective of accessing the internal knowledge bases of the compromised companies, the experts said. They quoted the cybersecurity section of an internet technology company as saying Lazarus has been targeting engineers and technical support employees "using malicious versions of open source applications."

In December 2022, the panel said, South Korea's national police agency announced that Kimsuky had targeted 892 foreign policy related experts "in an effort to steal personal data and email lists."

The police reported that the hackers didn't manage to steal sensitive information, but they "laundered IP addresses of the victims and employed 326 detour servers and 26 member states to make tracing difficult," the experts said. The police noted it was the first time they detected Kimsuky using ransomware, saying 19 servers and 13 businesses were affected, of which two paid 2.5 million South Korean won ($1,980) in Bitcoin to the hackers.

On military-related issues, the experts said they investigated the "apparent export" of military communications equipment from a North Korean company under U.N. sanctions to Ethiopia's defense ministry in June 2022.

The panel said it has not yet received a reply from Ethiopia's government about a photo published by the Ethiopian media in November allegedly showing a piece of equipment from the Global Communications Co., known as Glocom, being used by a top military official. Eritrea also hasn't responded to questions about its alleged procurement of Glocom equipment, the experts said.

North Korea may also have illegally traded arms and related material with a number of countries, including sending artillery shells, infantry rockets and missiles to Russia—claims Pyongyang and Moscow have consistently denied, the panel said. And the experts said they are investigating the reported sale of weapons from a North Korean company on the U.N. sanctions list to the Myanmar military through a Myanmar company.

Citation: UN experts: North Korean hackers stole record virtual assets (2023, February 8) retrieved 2 May 2024 from https://techxplore.com/news/2023-02-experts-north-korean-hackers-stole.html