Published on *The National Law Review* https://natlawreview.com

UK and Republic of Korea Issue Warning about DPRK State-Linked Cyber Actors

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On November 23, 2023, the UK government's National Cyber Security Centre ("NCSC") and the Republic of Korea's National Intelligence Service ("NIS") issued a joint advisory detailing techniques and tactics used by cyber actors linked to the Democratic People's Republic of Korea ("DPRK") that are carrying out software supply chain attacks. The publication follows the recent announcement of a new Strategic Cyber Partnership between the UK and the Republic of Korea where the two nations have committed to work together to tackle common cyber threats.

In the statement by the NCSC, it notes that DPRK state-linked cyber actors have been using increasingly sophisticated techniques to gain access to victims' systems. Particularly, the cyber actors have been observed leveraging zero-day vulnerabilities in third-party software to gain access to specific targets or indiscriminate organizations via their supply chains. The NCSC and the NIS consider these supply chain attacks to "help fulfil wider DPRK-state priorities, including revenue generation, espionage and the theft of advanced technologies." In addition to providing technical details about the malicious activity and tactics of the cyber actors, the joint statement also includes case studies of recent attacks emanating

from the DPRK and advice on how organizations can seek to mitigate supply chain compromises. The NCSC and NIS believe these attacks are likely to increase and therefore encourage organizations to follow the recommended actions in the joint advisory.

National Law Review, Volume XIII, Number 331