Varios grupos de amenazas cibernéticas vinculados a Corea del Norte (también conocida como la República Popular Democrática de Corea o RPDC) han sido relacionados con ataques dirigidos a organizaciones e individuos en el ámbito de Web3 y las criptomonedas.

> *"El interés en Web3 y las criptomonedas parece estar motivado principalmente por razones financieras debido a las fuertes sanciones impuestas a Corea del Norte",* señaló Mandiant (propiedad de Google) en su informe *M-Trends 2025*.

Estas actividades buscan generar ganancias económicas que, según informes, financian el programa de armas de destrucción masiva (ADM) y otros recursos estratégicos de Corea del Norte.

La firma de ciberseguridad indicó que los actores de amenazas ligados a Corea del Norte han desarrollado herramientas personalizadas escritas en lenguajes como Golang, C++ y Rust, capaces de infectar sistemas operativos Windows, Linux y macOS.

Al menos tres grupos de amenazas identificados como UNC1069, UNC4899 y UNC5342 han sido descubiertos apuntando a desarrolladores y comunidades relacionadas con blockchain y criptomonedas, principalmente para obtener acceso ilícito a billeteras digitales y las organizaciones donde trabajan.

Breve descripción de estos actores:

- UNC1069 (activo desde abril de 2018): utiliza técnicas de ingeniería social como invitaciones falsas a reuniones o suplantación de inversores en Telegram para acceder a activos digitales de sus víctimas.
- UNC4899 (activo desde 2022): ha realizado campañas disfrazadas de ofertas de trabajo para distribuir malware e incluso comprometer cadenas de suministro con fines económicos. Se superpone con grupos como Jade Sleet y TraderTraitor.
- UNC5342 (activo desde enero de 2024): engaña a desarrolladores con supuestas ofertas laborales que contienen malware. Comparte características con grupos como

DEV#POPPER y Famous Chollima.

Otro actor relevante es UNC4736, que ha atacado a la industria blockchain infectando aplicaciones de trading. Se le atribuye el ataque en cadena contra 3CX en 2023.

Mandiant también identificó a UNC3782, un grupo que lleva a cabo campañas masivas de phishing en el sector de criptomonedas. En 2023, robaron más de 137 millones de dólares en un solo día al atacar usuarios de TRON. En 2024, se enfocaron en usuarios de Solana con sitios web que vaciaban sus billeteras.

El robo de criptomonedas es solo uno de los métodos que Corea del Norte utiliza para evadir sanciones internacionales. Desde 2022, un grupo conocido como UNC5267 ha enviado miles de ciudadanos a trabajar de forma remota en empresas de EE. UU., Europa y Asia, principalmente desde China y Rusia.

Muchos de estos trabajadores están ligados al Buró General 313 del Departamento de la Industria de Municiones, responsable del programa nuclear norcoreano. Usan identidades robadas o completamente falsas y hasta tecnología deepfake en entrevistas laborales.

> *"Esto les da dos ventajas clave: pueden postular múltiples veces al mismo puesto con identidades distintas, y evitan ser detectados o fichados"*, explicó Evan Gordenker, de Palo Alto Networks.

Este esquema busca enviar los sueldos obtenidos a Pyongyang, mantener acceso prolongado a redes corporativas, y en ocasiones, extorsionar a los empleadores.

> *"Incluso han intensificado campañas de extorsión y se han infiltrado en escritorios virtuales, redes y servidores corporativos"*, añadieron Jamie Collier y Michael Barnhart del Grupo de Inteligencia de Amenazas de Google.

En 2024, Mandiant identificó a un trabajador norcoreano que utilizó al menos 12 identidades falsas para buscar empleo en EE. UU. y Europa. En un caso, dos identidades falsas compitieron por un mismo trabajo; uno de ellos fue contratado. En otro caso, cuatro trabajadores sospechosos fueron contratados por la misma empresa en un año.