El Ministerio de Seguridad del Estado de China (MSS) ha acusado a Estados Unidos de haber penetrado en los servidores de Huawei de forma ilícita, sustrayendo información crucial y insertando puertas traseras desde 2009, en medio de crecientes tensiones geopolíticas entre ambas naciones.

En un comunicado publicado en WeChat, la entidad gubernamental afirmó que las agencias de inteligencia estadounidenses han empleado *«todos los recursos posibles»* para llevar a cabo labores de vigilancia, robo encubierto e intrusiones en numerosos países alrededor del mundo, incluyendo China, utilizando un *«poderoso arsenal de ataques cibernéticos».* No se proporcionaron detalles concretos sobre las supuestas intrusiones.

De manera explícita, se señaló a la Operación de Red de Computadoras de la Agencia de Seguridad Nacional de Estados Unidos (NSA) (anteriormente conocida como la Oficina de Operaciones de Acceso Personalizado o TAO) como la responsable de llevar a cabo de forma reiterada ataques sistemáticos basados en plataformas contra el país, con el fin de saquear sus *«valiosos recursos de datos».*

El comunicado prosiguió afirmando que la unidad de inteligencia especializada en ciber-guerra y recolección de información había vulnerado los servidores de Huawei en 2009 y que había realizado *«decenas de miles de ataques maliciosos en red»* dirigidos hacia entidades nacionales, incluyendo la Universidad Politécnica del Noroeste, con el propósito de extraer información sensible, una acusación que China había planteado por primera vez en septiembre de 2022.

Adicionalmente, se reporta que el Centro Nacional de Respuesta de Emergencia a Virus de Computadora de China (NCVERC) habría aislado un artefacto de spyware denominado *«Second Date»* al lidiar con un incidente en la universidad pública de investigación, el cual supuestamente habría sido desarrollado por la NSA y operado de forma encubierta en *«miles de dispositivos de red en múltiples países alrededor del mundo».*

Información previamente difundida por el South China Morning Post y China Daily describe a Second Date como un malware versátil capaz de monitorear y tomar el control del tráfico de

red, además de inyectar código malicioso. Se cree que algunos de los países afectados por el spyware incluyen a Alemania, Japón, Corea del Sur, India y Taiwán.

El MSS argumenta que la agencia de inteligencia de Estados Unidos ha empleado este tipo de armamento y equipamiento a gran escala durante más de una década para llevar a cabo ciberataques y operaciones de espionaje cibernético contra China, Rusia y otras 45 naciones y regiones alrededor del mundo. Estas acciones, según el MSS, se han dirigido hacia sectores como las telecomunicaciones, la investigación científica, la economía, la energía y el ámbito militar.

Además, el MSS alega que Estados Unidos ha presionado a las empresas tecnológicas para que incorporen puertas traseras en su software y equipos con el propósito de llevar a cabo espionaje cibernético y robo de datos, mencionando ejemplos como las empresas X-Mode Social y Anomaly Six, las cuales han demostrado capacidad para rastrear los teléfonos móviles de sus usuarios.

El comunicado concluye señalando que durante mucho tiempo ha sido un secreto a voces que Estados Unidos ha dependido de sus ventajas tecnológicas para llevar a cabo operaciones de espionaje a gran escala en países de todo el mundo, incluyendo a sus aliados, y ha realizado actividades de robo cibernético. China, Rusia, Irán, China y Corea del Norte se presentan como los principales objetivos de estas acciones.

En julio de 2023, tras la revelación por parte de Microsoft de una campaña de espionaje vinculada a China llevada a cabo por un actor conocido como Storm-0558, dirigida a dos docenas de organizaciones en Estados Unidos y Europa, China respondió calificando a Estados Unidos como *«el mayor imperio de hackeo del mundo y el mayor ladrón cibernético global».*

El MSS hizo su debut en WeChat el 1 de agosto de 2023, resaltando la necesidad de fortalecer los esfuerzos contra el espionaje y alentar a los ciudadanos a reportar actividades sospechosas, ofreciendo recompensas y protección por sus contribuciones.