El Instituto de Investigación de Energía Atómica de Corea (KAERI), administrado por el estado de Corea del Sur, reveló este viernes que su red interna fue infiltrada por presuntos hackers que operan desde su contraparte del norte.

Al parecer, la intrusión tuvo lugar el 14 de mayo mediante una vulnerabilidad en un proveedor de red privada virtual (VPN) sin nombre, e involucró un total de 13 direcciones IP, una de las cuales, «27.102.114[.]89», ya se había vinculado a un actor de amenazas patrocinado por el estado apodado como Kimsuky.

KAERI, establecido en 1959 y ubicado en la ciudad de Daejeon, es un instituto de investigación financiado por el gobierno, que diseña y desarrolla tecnologías nucleares relacionadas con reactores, barras de combustible, fusión por radiación y seguridad nuclear.

Luego de la intrusión, el grupo de expertos dijo que tomó medidas para bloquear las direcciones IP del atacante en cuestión y aplicó los parches de seguridad necesarios a la solución VPN vulnerable.

> *«En la actualidad, el Instituto de Investigación de Energía Atómica está investigando el tema de la piratería y la cantidad de daño»,* dijo la entidad en un comunicado.

El desarrollo se produce después de un informe del SISA Journal, que reveló la violación de datos, afirmando que la agencia estaba tratando de encubrir el ataque al negar que dicho incidente tuvo lugar. KAERI lo atribuyó a un *«error en la respuesta del personal de nivel de trabajo».*

Activo desde 2012, Kimsuky, también conocido como Velvet Chollima, Black Banshee o Thallium, es un actor de amenazas norcoreano conocido por sus campañas de ciberespionaje dirigidas a grupos de expertos y operadores de energía nuclear en Corea del Sur.

A inicios del mes, la compañía de seguridad cibernética Malwarebytes, reveló una ola de ataques emprendidos por los hackers para atacar a funcionarios gubernamentales de alto

perfil en el país al instalar una puerta trasera de Android y Windows llamada AppleSeed para acumular información valiosa.

Las entidades objetivo incluyeron al Ministerio de Relaciones Exteriores, el Embajador de la Embajada de Sri Lanka ante el Estado, el Oficial de Seguridad Nuclear del Organismo Internacional de Energía Atómica (OIEA) y el Cónsul General Adjunto del Consulado General de Corea en Hong Kong, con la dirección IP mencionada antes utilizada para comunicaciones de comando y control (C2).

Aún no está claro qué vulnerabilidad de VPN se aprovechó para violar la red, pero cabe mencionar que los sistemas VPN sin parches de Pulse Secure, SonicWall, Fortinet FortiOS y Citrix han sido objetivo de ataques por parte de múltiples actores de amenazas en los últimos años.