Microsoft anunció el viernes que fue víctima de un ataque perpetrado por un Estado, dirigido a sus sistemas corporativos, que resultó en la sustracción de correos electrónicos y archivos adjuntos de altos ejecutivos y otras personas en los departamentos de ciberseguridad y legal de la empresa.

La compañía de Windows atribuyó el ataque a un grupo ruso de amenazas persistentes avanzadas (APT) al que rastrea con el nombre de Midnight Blizzard (anteriormente conocido como Nobelium), también identificado como APT29, BlueBravo, Cloaked Ursa, Cozy Bear y The Dukes.

Se indicó además que se tomaron medidas de manera inmediata para investigar, interrumpir y mitigar la actividad maliciosa desde su descubrimiento el 12 de enero de 2024. Se estima que la campaña comenzó a fines de noviembre de 2023.

> *«El actor de amenazas utilizó un ataque de rociado de contraseñas para comprometer una cuenta heredada de prueba que no estaba en producción, logrando un punto de apoyo. Posteriormente, empleó los permisos de dicha cuenta para acceder a un porcentaje muy reducido de las cuentas de correo electrónico corporativas de Microsoft, incluyendo miembros de nuestro equipo de liderazgo senior y empleados en áreas como ciberseguridad, legal y otras funciones. Fue en este punto donde se extrajeron algunos correos electrónicos y documentos adjuntos»*, detalló Microsoft.

Redmond señaló que la naturaleza del objetivo sugiere que los actores de amenazas buscaban acceder a información relacionada con ellos mismos. También se destacó que el ataque no surgió como resultado de alguna vulnerabilidad de seguridad en sus productos, y no hay evidencia de que el adversario haya accedido a entornos de clientes, sistemas de producción, código fuente o sistemas de inteligencia artificial.

No obstante, el gigante de la informática no divulgó cuántas cuentas de correo electrónico fueron comprometidas ni qué información fue accesada, pero informó que estaba en proceso

de notificar a los empleados afectados como resultado del incidente.

El grupo de piratería, anteriormente responsable del compromiso de la cadena de suministro de SolarWinds, ha apuntado a Microsoft en dos ocasiones: primero, en diciembre de 2020, para extraer código fuente relacionado con Azure, Intune y componentes de Exchange, y luego, en junio de 2021, comprometiendo tres de sus clientes mediante ataques de rociado de contraseñas y fuerza bruta.

> *«Este ataque resalta el riesgo continuo que representan los actores de amenazas respaldados por Estados-nación con abundantes recursos, como Midnight Blizzard, para todas las organizaciones»,* afirmó el Centro de Respuesta de Seguridad de Microsoft (MSRC).