Cientos de bases de datos en Amazon Relational Databases Service (Amazon RDS) están exponiendo información de identificación personal (PII), según los nuevos hallazgos de Mitiga, una empresa de respuesta a incidentes en la nube.

> *«La filtración de PII de esta forma proporciona un tesoro potencial para los atacante, ya sea durante la fase de reconocimiento de la cadena de eliminación cibernética o las campañas de extorsión/ransomware»,* dijeron los investigadores Ariel Szarf, Doron Karmi y Lionel Saposnik en un informe.

Esto incluye nombres, direcciones de correo electrónico, números de teléfono, fechas de nacimiento, estado civil, información de alquiler de automóviles e incluso inicios de sesión de la empresa.

Amazon RDS es un servicio web que permite configurar bases de datos relacionales en la nube de Amazon Web Services (AWS). Ofrece soporte para distintos motores de bases de datos como MariaDB, MySQL, Oracel, PostgreSQL y SQL Server.

La causa principal de las fugas se deriva de una función llamada instantáneas públicas de RDS, que permite crear una copia de seguridad de todo el entorno de la base de datos que se ejecuta en la nube y todas las cuentas de AWS pueden acceder a ella.

> *«Al compartir una instantánea como pública, asegúrese de que ninguna de su información privada esté incluida en la instantánea pública. Cuando una instantánea se comparte públicamente, todas las cuentas de AWS tienen permiso para copiar y crear instancias de bases de datos a partir de ella»,* dice Amazon en su documentación.

La compañía israelí, que llevó a cabo la investigación del 21 de septiembre de 2022 al 20 de octubre de 2022, dijo que encontró 810 instantáneas que se compartieron públicamente por

una duración variable, desde unas pocas horas hasta semanas, lo que las hace propicias para el abuso por parte de hackers.

De las 810 instantáneas, más de 250 de las copias de seguridad estuvieron expuestas durante 30 días, lo que sugiere que probablemente se olvidaron.

Según la naturaleza de la información expuesta, los atacantes podrían robar los datos para obtener ganancias financieras o aprovecharlos para comprender mejor el entorno de TI de una empresa, lo que después podría actuar como un trampolín para los esfuerzos de recopilación de inteligencia encubierta.

Se recomienda encarecidamente que las instantáneas de RDS no sean de acceso público para evitar posibles fugas o mal uso de datos confidenciales o cualquier otro tipo de amenaza a la seguridad. También es necesario cifrar las instantáneas cuando corresponda.