Un pirata informático desconocido se infiltró en 22,900 bases de datos MongoDB inseguras, borrando su contenido y dejando una nota de rescate que exige bitcoin a cambio de los datos. En caso de que no se pague el rescate en dos días, amenaza con notificar a las autoridades a cargo de hacer cumplir el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

El hacker utiliza secuencias de comandos automatizadas para buscar en Internet las instalaciones de MongoDB en Internet sin protección por contraseña, luego elimina el contenido y solicita 0.015 BTC, equivalentes a unos 140 dólares, para devolver los datos.

El pirata informático incluso proporcionó una guía sobre cómo comprar bitcoin. Parece ser que el ciberdelincuente utiliza múltiples billeteras bitcoin y direcciones de correo electrónico, pero la redacción de la amenaza es consistente.

Victor Gevers, investigador de seguridad cibernética de la Fundación GDI, dijo que los primeros ataques carecían de la función de borrado de datos. Una vez que el delincuente se dio cuenta del error en su script, lo modificó y comenzó a borrar las bases de datos MongoDB. Se han registrado ataques con esta nota de rescate desde abril de 2020.

El investigador declaró que notó los sistemas borrados mientras revisaba las bases de datos MongoDB que se suponía que debía informar para poder protegerse. *«Hoy, solo pude reportar una fuga de datos. Normalmente, puedo hacer al menos entre 5 o 10»*, dijo.

Aunque el rescate exigido puede parecer una suma pequeña, al multiplicarlo por las bases de datos inseguras, el monto ronda los 3.2 millones de dólares en total. Y aunque por lo general nadie accede a pagar un rescate, para muchos resultaría mejor eso que pagar una multa por violación a las leyes GDPR.