Una base de datos del foro de webmasters de Digital Point, resultó afectada con la filtración de los registros de más de 800 mil usuarios.

Digital Point, con sede en San Diego, California, se describe a sí misma como *«la comunidad de webmasters más grande del mundo»,* que reúne a distintos especialistas y profesionales.

El 1 de julio, el equipo de investigación de WebsitePlanet y el investigador Jeremiah Fowler, descubrieron una base de datos de Elasticsearch no segura, que contiene más de 62 millones de registros. En total, los datos pertenecientes a 863,412 usuario de Digital Point se incluyeron en la filtración.

Según el equipo de investigación, los nombres, las direcciones de correo electrónico y números de identificación de usuario internos, se pusieron a disposición del público.

Además, los registros internos y los detalles de las publicaciones de los usuarios se almacenaron en la base de datos abierta.

Al examinar la base de datos para averiguar quién era el propietario, los investigadores encontraron conjuntos de datos relacionados con los miembros del foro que marcaron publicaciones y las razones detrás de estos informes, incluidas las acusaciones de *«malos tratos comerciales»*, spam y otras razones.

Además de las ramificaciones de seguridad habituales del robo de datos de los usuarios y el phishing, la base de datos podría haberse convertido en una de las muchas que sucumbieron a Meow Bot, un script automatizado que fue responsable del compromiso de miles de bases de datos de MongoDB y Elasticsearch no seguras en julio. Una vez que se ha implementado el script, anula los datos con números y la palabra «meow».

> *«Uno de los peligros de una base de datos no protegida por contraseña es que es un objetivo que espera ser robado, cifrado o eliminado»*, dijeron los investigadores.

Fowler envió un aviso de divulgación responsable a Digital Point el 1 de julio, el mismo día en que se descubrió la fuga de datos, a través de una dirección de correo electrónico adecuada que se encuentra en la base de datos. La alerta se tomó en serio y el acceso a la base de datos se revocó en cuestión de horas.

Sin embargo, el foro no se comunicó con los investigadores para responder a las solicitudes de seguimiento.