Más de 2,200 millones de datos personales, entre los que destacan nombres de usuario y contraseñas, han sido filtrados a Internet para su descarga gratuita.

Según Wired, los investigadores descubrieron una base de datos de 845 GB conocida como Collection #2-5. Esto ocurre a unas semanas de haberse revelado la filtración denominada como Collection #1, que se consideraba como la filtración más grande de la historia con 773 millones de correos electrónicos expuestos.

Collection #2-5 tiene 25 mil millones de entradas, muchas repetidas, pero 611 millones son únicas y no aparecen en la filtración anterior. Los investigadores del Hasso Plattner de Postdam, Alemania, afirman que la cifra total de nombres de usuario únicos y contraseñas contenidos en las colecciones 1 a 5 asciende a los 2,200 millones.

El compilado Collection #2-5 ha sido descargado desde los fotos de hackers por medio de enlaces a Mega o archivos torrent. Los expertos dijeron que muchos de los datos no son nuevos, ya que se originaron de hackeos masivos a empresas como Yahoo, LinkedIn o Adobe. Parte de la información vulnerada también vendría de sitios más pequeños o fotos que son atacados.

Según los expertos, estos archivos ya perdieron su valor, razón por la que ahora se ofrecen de forma libre. Posiblemente, Collection #1-5 cuente con datos de acceso a Last.fm o Dropbox, que fueron hackeados en 2012, al igual que contraseñas DailyMotion, hackeada en 2016.

Aunque se trate de datos viejos, no deja de ser un problema importante, ya que muchos usuarios utilizan las mismas contraseñas por mucho tiempo, lo que podría hacer que los piratas informáticos utilicen los datos para tratar de acceder a otros servicios.

El Instituto Hasso Plattner liberó una herramienta en la que se puede verificar si tu correo electrónico se encuentra en las filtraciones Collection #1-5, así como en otros ataques por parte de hackers. Al introducir tu correo en esta herramienta, recibirás un correo con el listado de sitios afectados y el tipo de información personal que fue expuesta.

Se recomienda que los usuarios cambien sus contraseñas y preferiblemente, utilizar contraseñas diferentes en cada servicio, además de utilizar la autenticación de dos factores.