02/06/2024

Hackers filtran contraseñas de Llave CDMX y arriesgan a 6.3 millones de usuarios



En grupos de mensajería cifrada, ciberatacantes anónimos han filtrado archivos que revelan usuarios y contraseñas de capitalinos que usan la principal plataforma para la gestión digital de trámites y servicios de la **Ciudad de México**: Llave CDMX Expediente.

Según el mismo sitio, gestionado por la Agencia Digital de Innovación Pública (ADIP), más de 6.3 millones de usuarios utilizan este sistema para realizar trámites como la **licencia digital para conducir, Mi Beca para Empezar, la tarjeta de circulación vehicular, denuncias digitales** entre muchos más.

El problema es que, además de los accesos, cualquier persona que tenga las contraseñas, ya compartidas en los grupos mencionados, puede acceder a datos personales del usuario, como **nombre completo, CURP, correo electrónico, fecha de nacimiento y número de celular**. Además, pueden descargar todos los documentos gestionados por el usuario en su cuenta personal.

Víctor Ruiz, socio fundador de la empresa de ciberseguridad SILIKN, realizó la advertencia y recomendó a los usuarios de la plataforma que cambien sus contraseñas de manera urgente e inmediata. “El gobierno de la CDMX, una vez más, ha demostrado su ineficiencia en el resguardo de datos personales”, advirtió.

Cabe reiterar que las credenciales de la plataforma están accesibles a través de canales de mensajería cifrada, y aunque no se han expuesto públicamente, algunos delincuentes han ofrecido ejemplos de la información que poseen de manera clandestina.

Publimetro México comprobó, con fines meramente periodísticos, que las credenciales filtradas son funcionales y revelan información privada de usuarios de la Ciudad de México, evidenciando todo su historial de descarga de documentos, incluidos **fotocívicas, seguro de desempleo, constancias de antecedentes no penales y actas digitales del registro civil** , entre muchos otros.

Para dimensionar el impacto del uso de esta plataforma, cabe señalar que solo en **2023** se realizaron **1.5 millones** de trámites de licencia digital para conducir, **1.2 millones** de Mi Beca para Empezar, **1.1 millones** de tarjetas de circulación vehicular y **639,787** denuncias digitales.

Hackeos en la Ciudad de México

En los últimos meses, se han intensificado los ciberataques contra diversas dependencias tanto del gobierno federal como del local. Uno de los ejemplos más notorios es el caso conocido como “Chilango Leaks,” en el que un hacker apodado Lord Peña extrajo 2.3

millones de correos electrónicos del gobierno de la **Ciudad de México**.

En este ataque, **Lord Peña** obtuvo más de 2 terabytes de información de aproximadamente **2,300 cuentas** de correo de funcionarios de distintas dependencias. Aunque inicialmente intentó vender dicha información, finalmente el hacker optó por hacer pública la filtración de datos.

Otro caso reciente involucra un ataque perpetrado por el hacker Pancho Villa, miembro del grupo conocido como **Mexican Mafia**, al sitio oficial de la **alcaldía Iztapalapa**, logrando acceso completo al servidor. Hasta el martes 21 de mayo, el sitio sigue sin poder ser restablecido.

¿Para qué se creo Llave CDMX Expediente?

De acuerdo con la **ADIP**, con esta iniciativa se valida la identidad de las personas utilizando autenticación con medios oficiales, lo que ayuda a mitigar el fraude y los riesgos de mal uso de la identidad. Además, la agencia señala que con la llave se crea una huella digital a partir de todas las interacciones realizadas, lo que permite a las personas ahorrar tiempo y dinero al no tener que acudir personalmente a las oficinas o perder días laborales.

ADIP investiga el incidente

Tras la divulgación de la noticia sobre la vulneración, **Eduardo Clark**, titular de la ADIP, afirmó a **Víctor Ruiz** que no hay contraseñas fáciles de descifrar y que el acceso sería imposible. Sin embargo, **Publimetro México** confirmó que dichas credenciales de acceso sí están operativas.

Fuente: www.publimetro.com.mx

LINK DE LA NOTICIA