Una compañía líder en tecnología web, y dos de sus subsidiarias, sufrieron una violación masiva de datos, afectando a millones de clientes de todo el mundo que han comprado dominios.

Los principales registradores de dominios del mundo, Web.com, Network Solutions y Register.com, revelaron una violación de seguridad que puede haber resultado en el robo de la información de la cuenta de los clientes.

Fundada en 1999 y con sede en Jacksonville, florida, Web.com es una compañía líder en tecnología web que posee Network Solutions y Register.com. Las compañías ofrecen servicios web como alojamiento web, diseño de sitios web y marketing en línea para ayudar a las personas a crear sus sitios web.

A fines de agosto de 2019, una tercera persona tuvo acceso no autorizado a un *«número limitado»* de los sistemas informáticos de la compañía, y según los informes obtenidos, accedió a millones de registros de cuentas de clientes actuales y anteriores con Web.com, Network Solutions y Register.com.

La compañía dijo que se enteró de la intrusión de seguridad solo el 16 de octubre de 2019, pero no reveló ningún detalle sobre cómo ocurrió el incidente.

Según los registradores de dominios afectados, la información robada incluye datos de contacto de sus clientes, como:

- Nombres
- Direcciones
- Números de teléfono
- Correos electrónicos
- Información sobre los servicios ofrecidos al cliente

Las compañías también confirmaron que ninguna información de tarjeta de crédito se vio comprometida como resultado del incidente de violación de seguridad, ya que afirman cifrar

los números de tarjeta de crédito de sus clientes antes de almacenarlos en sus bases de datos.

> *«Almacenamos los números de tarjeta de crédito en un estándar de cifrado que cumple con PCI (industria de tarjetas de pago) y no creemos que la información de su tarjeta de crédito sea vulnerable como resultado específico de este incidente»*, dice el aviso de incumplimiento publicado en los sitios web de Web.com, Network Solutions y Register.com.

Cabe mencionar que las contraseñas para los inicios de sesión de las cuentas de los clientes afectados tampoco se vieron comprometidas, lo que de otra forma podría haber permitido a los atacantes secuestrar de forma permanente los nombres de dominio al transferirlos a una cuenta propiedad de los atacantes con un servicio separado.

Las compañías tomaron las medidas necesarias para detener la intrusión de seguridad en el momento del descubrimiento e inmediatamente iniciaron una investigación al involucrar a una firma líder independiente de seguridad cibernética para determinar el alcance del incidente.

Las compañías también notificaron a todas las autoridades relevantes y ya comenzaron a trabajar con la policía federal.

Los tres registradores de dominios afectados también están en proceso de contactar a los clientes afectados por correo electrónico y por medio de sus sitios web.

Como una medida de precaución, se recomienda a los clientes afectados que cambien las contraseñas de sus cuentas de Web.com, Network Solutions y Register.com y de cualquer otra cuenta en línea donde se utilicen las mismas contraseñas.

> *«Ya hemos tomado medidas adicionales para asegurar su cuenta, y no hay nada*

> *que deba hacer en este momento. La próxima vez que inicie sesión en su cuenta, se le pedirá que restablezca su contraseña»,* dice la compañía.

Debido a que los datos expuestos incluyen información de identificación personal (PII), los clientes afectados deben sospechar principalmente de los correos electrónicos de phishing, que generalmente son el siguiente paso de los delincuentes informáticos en un intento de engañar a los usuarios para que revelen sus contraseñas y la información de su tarjeta de crédito.

Esta no es la primera vez que Web.com revela un incidente de seguridad. En agosto de 2015, la compañía sufrió una violación de datos que comprometió la información personal y tarjetas de crédito de casi 93 mil clientes.