



Dropbox revela una violación del servicio de firma digital que afecta a todos sus usuarios

El proveedor de servicios de almacenamiento en la nube Dropbox informó el miércoles que Dropbox Sign (antes conocido como HelloSign) fue comprometido por actores de amenazas no identificados, quienes accedieron a correos electrónicos, nombres de usuario y configuraciones generales de cuenta asociadas con todos los usuarios del producto de firma digital.

En una presentación ante la Comisión de Valores y Bolsa de Estados Unidos (SEC), la compañía [reveló](#) que se enteró de este «acceso no autorizado» el 24 de abril de 2024. Dropbox había anunciado sus planes de adquirir HelloSign en enero de 2019.

«El actor de amenazas logró acceder a datos de todos los usuarios de Dropbox Sign, como direcciones de correo electrónico y nombres de usuario, así como ajustes generales de cuenta», se indicó en la [presentación](#) del Formulario 8-K.

«Además, para algunos grupos de usuarios, el actor de amenazas también obtuvo acceso a números de teléfono, contraseñas encriptadas y cierta información de autenticación, como claves de API, tokens de OAuth y autenticación multifactor».

Lo que es aún más preocupante, es que la intrusión también afecta a terceros que recibieron o firmaron un documento a través de Dropbox Sign, pero que nunca crearon una cuenta, exponiendo específicamente sus nombres y direcciones de correo electrónico.

Hasta ahora, la investigación no ha encontrado evidencia de que los atacantes hayan accedido al contenido de las cuentas de los usuarios, como acuerdos o plantillas, ni a su información de pago. Se ha señalado que el incidente se limita a la infraestructura de Dropbox Sign.

Se presume que los atacantes obtuvieron acceso a una herramienta de configuración automatizada de Dropbox Sign y comprometieron una cuenta de servicio que forma parte del backend de Sign, aprovechando los privilegios elevados de la cuenta para acceder a la base



Dropbox revela una violación del servicio de firma digital que afecta a todos sus usuarios

de datos de clientes.

Sin embargo, la compañía no reveló cuántos clientes se vieron afectados por el ataque, pero aseguró que está en proceso de contactar a todos los usuarios afectados y proporcionar «*instrucciones paso a paso*» para proteger su información.

«*Nuestro equipo de seguridad también ha restablecido las contraseñas de los usuarios, ha cerrado la sesión de los usuarios en todos los dispositivos conectados a Dropbox Sign y está coordinando la rotación de todas las claves de API y tokens de OAuth*», afirmó la compañía.

Dropbox también informó que está cooperando con las autoridades policiales y reguladoras en relación con este asunto. Se está llevando a cabo un análisis más detallado del incidente.

Este ataque representa el segundo incidente de seguridad que afecta a Dropbox en los últimos dos años. En noviembre de 2022, la compañía reveló que fue víctima de una campaña de phishing que permitió que actores de amenazas no identificados obtuvieran acceso no autorizado a 130 de sus repositorios de código fuente en GitHub.