El servicio de alojamiento de archivos Dropbox reveló el martes que fue víctima de una campaña de phishing que permitió a actores de amenazas no identificados obtener acceso no autorizado a 130 de sus repositorios de código fuente en GitHub.

> *«Estos repositorios incluían nuestras propias copias de bibliotecas de terceros ligeramente modificadas para su uso por Dropbox, prototipos internos y algunas herramientas y archivos de configuración utilizados por el equipo de seguridad»,* dijo la compañía en un aviso.

La violación de seguridad resultó en el acceso a algunas claves de API utilizadas por los desarrolladores de Dropbox, así como a *«unos pocos miles de nombres y direcciones de correo electrónico pertenecientes a empleados de Dropbox, clientes actuales y anteriores, clientes potenciales de ventas y proveedores».*

Sin embargo, enfatizó que los repositorios no contenían código fuente relacionado con sus aplicaciones o infraestructura principales.

Dropbox, que ofrece servicios de almacenamiento en la nube, copia de seguridad de datos y firma de documentos, entre otros, tiene más de 17.37 millones de usuarios de pago y 700 millones de usuarios registrados en agosto de 2022.

La divulgación se produce más de un mes después de que tanto GitHub como CircleCI advirtieran sobre ataques de phishing diseñados para robar credenciales de GitHub por medio de notificaciones falsas que pretendían ser de la plataforma CI/CD.

La firma con sede en San Francisco dijo que *«múltiples usuarios de Dropbox recibieron correos electrónicos de phishing que se hacían pasar por CircleCI»* a inicios de octubre, algunos de los cuales se deslizaron a través de sus filtros automatizados de correo no deseado para llegar a las bandejas de entrada de correo electrónico de los empleados.

> *«Estos correos electrónicos de aspecto legítimo dirigían a los empleados a visitar una página de inicio de sesión falsa de CircleCI, ingresar su nombre de usuario y contraseña de GitHub y luego usar su clave de autenticación de hardware para pasar una contraseña de un solo uso (OTP) al sitio malicioso»,* dijo Dropbox.

La compañía no reveló cuántos de sus empleados cayeron en el ataque de phishing, pero dijo que tomó medidas inmediatas para rotar todas las credenciales de desarrollador expuestas y que alertó a las autoridades policiales.

También dijo que no encontró evidencia de que se robaron datos de clientes como resultado del incidente, y agregó que está actualizando sus sistemas de autenticación de dos factores para admitir claves de seguridad de hardware para la resistencia al phishing.

> *«Incluso el profesional más escéptico y vigilante puede ser víctima de un mensaje cuidadosamente elaborado y entregado de la manera correcta en el momento adecuado. Esta es precisamente la razón por la que el phishing sigue siendo tan efectivo»*, agregó la compañía.

La notificación de Dropbox también se produce cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), publicó una guía para implementar la autenticación multifactor (MFA) resistente al phishing para protegerse contra el phishing y otras amenazas cibernéticas conocidas.

> *«Si una organización que usa MFA móvil basado en notificaciones push no puede implementar MFA resistente al phishing, CISA recomienda usar coincidencias de números para mitigar la fatiga de MFA»,* dijo la agencia.