Una compañía de desarrollo de software llamada Retool ha informado que las cuentas de 27 de sus clientes en la nube fueron vulneradas tras sufrir un ataque de ingeniería social dirigido y basado en mensajes de texto (SMS).

La empresa con sede en San Francisco atribuyó a una característica de sincronización en la nube de Google Account, introducida recientemente en abril de 2023, la agravación de la brecha, denominándola un *«patrón oscuro».*

> Snir Kodesh, el jefe de ingeniería de Retool, comentó: *«La circunstancia de que Google Authenticator se sincronice con la nube representa un vector de ataque inédito. Inicialmente, habíamos implementado la autenticación multifactor. No obstante, gracias a esta actualización de Google, lo que antes constituía autenticación multifactor pasó inadvertidamente (para los administradores) a ser una autenticación de un solo factor».*

Retool afirmó que el incidente tuvo lugar el 27 de agosto de 2023 y no permitió el acceso no autorizado a cuentas gestionadas en las instalaciones ni en las cuentas gestionadas por la empresa. Además, coincidió con la migración de las credenciales de inicio de sesión de la compañía a Okta.

El incidente se originó con un ataque de phishing mediante SMS dirigido a sus empleados, en el que los actores de amenazas se hicieron pasar por un miembro del equipo de TI y dieron instrucciones a los destinatarios para hacer clic en un enlace aparentemente legítimo con el fin de abordar un problema relacionado con la nómina.

Uno de los empleados cayó en la trampa del phishing, lo que lo llevó a una página de destino falsa que lo engañó para que proporcionara sus credenciales. En la siguiente fase del ataque, los hackers llamaron al empleado, nuevamente haciéndose pasar por un miembro del equipo de TI al manipular su «voz real» para obtener el código de autenticación multifactor (MFA).

> Kodesh señaló: *«El token adicional OTP compartido por teléfono fue crucial, ya que permitió al atacante agregar su propio dispositivo personal a la cuenta de Okta del empleado, lo que les permitió generar su propio MFA de Okta a partir de ese momento. Esto les permitió tener una sesión activa de G Suite [ahora Google Workspace] en ese dispositivo».*

El hecho de que el empleado también hubiera habilitado la función de sincronización en la nube de Google Authenticator permitió que los actores de amenazas obtuvieran un acceso elevado a los sistemas administrativos internos y tomaran el control efectivo de las cuentas pertenecientes a 27 clientes de la industria de las criptomonedas.

Los atacantes finalmente cambiaron las direcciones de correo electrónico de esos usuarios y restablecieron sus contraseñas. Fortress Trust, una de las empresas afectadas, experimentó el robo de cerca de $15 millones en criptomonedas como resultado del hackeo, según informó CoinDesk.

> Kodesh destacó: *«Debido a que el control de la cuenta de Okta llevó al control de la cuenta de Google, lo que a su vez llevó al control de todos los OTP almacenados en Google Authenticator».*

Este sofisticado ataque demuestra que la sincronización de códigos de un solo uso en la nube puede comprometer el factor *«algo que el usuario tiene»*, lo que requiere que los usuarios dependan de llaves de seguridad de hardware compatibles con FIDO2 o contraseñas para protegerse contra los ataques de phishing.

Aunque no se reveló la identidad exacta de los hackers, el modus operandi presenta similitudes con un actor de amenazas con motivaciones financieras conocido como Scattered Spider (también conocido como UNC3944), que es reconocido por sus tácticas avanzadas de phishing.

La utilización de deepfakes y medios sintéticos también ha sido objeto de una nueva advertencia por parte del gobierno de EE. UU., que advierte que los deepfakes de audio, video y texto pueden ser empleados para una amplia variedad de propósitos maliciosos, incluyendo ataques de compromiso empresarial por correo electrónico (BEC) y estafas de criptomonedas.