La plataforma de participación del cliente, Twilio, reveló el lunes que un hacker *«sofisticado»* obtuvo acceso no autorizado utilizando una campaña de phishing basada en SMS dirigida a su personal para obtener información acerca de un *«número limitado»* de cuentas.

El ataque de ingeniería social estaba empeñado en robar las credenciales de los empleados, dijo la compañía, llamando al atacante aún no identificado como *«bien organizado y metódico en sus acciones».* El incidente salió a la luz el 4 de agosto.

> *«Este ataque de base amplia contra nuestra base de empleados logró engañar a algunos empleados para que proporcionaran sus credenciales. Los atacantes después usaron las credenciales robadas para obtener acceso a algunos de nuestros sistemas internos, donde pudieron acceder a ciertos datos de los clientes»,* dijo la compañía.

La compañía tiene 268,000 cuentas de clientes activas y entre sus clientes destacan Airbnb, Box, Dell, DoorDash, eBay, Glassdoor, Lyft, Salesforce, Stripe, Twitter, Uber, VMware, Yelp y Zendesk. También posee el popular servicio de autenticación de dos factores (2FA) Authy.

Twitter, que sigue su investigación sobre el ataque, dijo que está trabajando directamente con los clientes que se vieron afectados. No reveló la escala del ataque, la cantidad de cuentas de empleados que se vieron comprometidas o a qué tipo de datos se pudo haber accedido.

Se sabe que los esquemas de phishing, que aprovechan tanto el correo electrónico como los SMS, se basan en tácticas de miedo agresivas para obligar a las víctimas a entregar su información confidencial.

Al parecer, los mensajes SMS se enviaron a empleados actuales y anteriores haciéndose pasar por su departamento de TI, atrayéndolos con notificaciones de caducidad de contraseña para hacer clic en enlaces maliciosos.

Las URL incluían palabras como «Twilio», «Okta» y «SSO» para aumentar las posibilidades de éxito y redirigir a las víctimas a un sitio web falso que suplantaba la página de inicio de sesión de la empresa. No está claro si las cuentas afectadas estaban protegidas con 2FA.

Twilio dijo que los mensajes se originaron en las redes de los operadores de Estados Unidos y que trabajó con el servicio de telecomunicaciones y los proveedores de alojamiento para cerrar el esquema y la infraestructura de ataque utilizada en la campaña. Sin embargo, los esfuerzos de eliminación se vieron contrarrestados por la migración de los atacantes a otros operadores y proveedores de alojamiento.

> *«Además, los atacantes parecían tener habilidades sofisticadas para hacer coincidir los nombres de los empleados de las fuentes con sus números de teléfono»,* dijo.

Desde entonces, la firma con sede en San Francisco, revocó el acceso a las cuentas de los empleados comprometidos para mitigar el ataque, y agregó que está examinando medidas de seguridad técnicas adicionales como medida preventiva.

La divulgación llega cuando el phishing continuo sigue siendo una gran amenaza que enfrentan las empresas. El mes pasado, se supo que el hackeo de 620 millones de dólares en Axie Infinity, fue la consecuencia de que uno de sus ex empleados fue engañado por una oferta de trabajo fraudulenta en LinkedIn.