Twilio, que a inicios del mes se convirtió en un sofisticado ataque de phishing, reveló la semana pasada que los atacantes también lograron acceder a las cuentas de 93 usuarios individuales de su servicio Authy de autenticación de dos factores (2FA).

La compañía de herramientas de comunicación dijo que el acceso no autorizado hizo posible que el atacante registrara dispositivos adicionales en esas cuentas. Desde entonces, identificó y eliminó los dispositivos agregados de forma ilegítima de las cuentas afectadas.

Authy, adquirida por Twilio en febrero de 2015, permite proteger las cuentas en línea con una segunda capa de seguridad para evitar ataques de apropiación de cuentas. Se estima que tiene casi 75 millones de usuarios.

Twilio dijo también que su investigación al 24 de agosto de 2022 arrojó 163 clientes afectados, frente a los 125 que informó el 10 de agosto, cuyas cuentas, dijo, fueron hackeadas durante un período de tiempo limitado.

Además de Twilio, se cree que la campaña en expansión, denominada Oktapus por Group-IB, afectó a 136 empresas, incluyendo Klaviyo, MailChimp, y un ataque fallido contra Cloudflare que fue frustrado por el uso de tokens de seguridad de hardware por parte de la empresa.

Las empresas objetivo abarcan los sectores de tecnología, telecomunicaciones y criptomonedas, con la campaña empleando un kit de phishing para capturar nombres de usuario, contraseñas y contraseñas de un solo uso (OTP) por medio de páginas de inicio no autorizadas que imitaban las páginas de autenticación de Okta de las respectivas organizaciones.

Después, los datos se canalizaron en secreto a una cuenta de Telegram controlada por los ciberdelincuentes en tiempo real, lo que permitió al actor de amenazas pivotar y apuntar a otros servicios en lo que se denomina un ataque a la cadena de suministro dirigido a DigitalOcean, Signal y Okta, ampliando efectivamente el alcance y escala de las intrusiones.

En total, se cree que la expedición de phishing le proporcionó al atacante al menos 9931

credenciales de usuario y 5441 códigos de autenticación de múltiples factores.

Okta por su parte, confirmó que el robo de credenciales tuvo un efecto dominó, lo que resultó en el acceso no autorizado a una pequeña cantidad de números de teléfonos móviles y mensajes SMS asociados que contenían OTP por medio de la consola administrativa de Twilio.

Al afirmar que las OTP tienen un período de validez de cinco minutos, Okta dijo que el incidente involucró al atacante buscando directamente 38 números de teléfono únicos en la consola, casi todos pertenecientes a una sola entidad, con el objetivo de expandir su acceso.

> *«El actor de amenazas usó credenciales previamente robadas en campañas de phishing para desencadenar desafíos de MFA basados en SMS, y usó el acceso a los sistemas Twilio para buscar contraseñas de un solo uso enviadas en esos desafíos»,* dijo Okta.

Okta, que está rastreando al grupo de hackers bajo el nombre de Scatter Swine, reveló además que su análisis de los registros de incidentes *«descubrió un evento en el que el actor de amenazas probó con éxito esta técnica contra una sola cuenta no relacionada con el objetivo principal».*

Al igual que en el caso de Cloudflare, el proveedor de gestión de identidad y acceso (IAM) reiteró que está al tanto de varios casos en los que el atacante envió una ráfaga de mensajes SMS dirigidos a los empleados y sus familiares.

> *«Es probable que el actor de amenazas obtenga números de teléfonos móviles de los servicios de agregación de datos disponibles comercialmente que vinculan los números de teléfono con los empleados de organizaciones específicas»,* dijo Okta.

Otra víctima de la cadena de suministro de la campaña es el servicio de entrega de alimentos

DoorDash, dijo que detectó *«actividad inusual y sospechosa de la red informática de un proveedor externo»,* lo que llevó a la compañía a desactivar el acceso del proveedor a su sistema para contener la violación.

Según la empresa, el allanamiento permitió al atacante acceder a nombres, direcciones de correo electrónico, direcciones de entrega y números de teléfono asociados con un *«pequeño porcentaje de personas».* En casos seleccionados, también se accedió a la información básica del pedido y a la información de la tarjeta de pago parcial.

DoorDash, que ha notificado directamente a los usuarios afectados, dijo que la parte no autorizada también obtuvo los nombres y números de teléfono o direcciones de correo electrónico de los repartidores (también conocidos como Dashers), pero enfatizó que no se accedió a las contraseñas, números de cuentas bancarias y números de seguro social.

La compañía con sede en San Francisco no divulgó detalles adicionales sobre quién es el proveedor externo, pero le dijo a TechCrunch que la violación está relacionada con la campaña de phishing 0ktapus.