Se ha identificado un nuevo conjunto de herramientas de phishing que simula las páginas de inicio de sesión de servicios de criptomonedas conocidos como parte de un grupo de ataques denominado CryptoChameleon, cuyo objetivo principal es atacar principalmente a dispositivos móviles.

> Según un informe de Lookout, *«este conjunto de herramientas permite a los atacantes crear réplicas exactas de las páginas de inicio de sesión único (SSO), utilizando una combinación de phishing a través de correo electrónico, SMS y llamadas de voz para engañar al objetivo y hacer que comparta nombres de usuario, contraseñas, URL de restablecimiento de contraseña e incluso fotos de identificación con cientos de víctimas, en su mayoría en los Estados Unidos».*

El kit de phishing apunta a empleados de la Comisión Federal de Comunicaciones (FCC), así como a usuarios de criptomonedas en plataformas como Binance, Coinbase, Gemini, Kraken, ShakePay, Caleb & Brown y Trezor. Hasta la fecha, se ha logrado engañar exitosamente a más de 100 víctimas.

Las páginas de phishing están diseñadas de tal manera que la pantalla falsa de inicio de sesión solo se muestra después de que la víctima completa una prueba CAPTCHA utilizando hCaptcha, evitando así que las herramientas de análisis automatizado detecten los sitios.

En algunos casos, estas páginas se distribuyen a través de llamadas telefónicas y mensajes de texto no solicitados, haciendo pasar al equipo de soporte al cliente de una empresa bajo el pretexto de asegurar la cuenta después de un supuesto hackeo.

Una vez que el usuario ingresa sus credenciales, se le solicita proporcionar un código de autenticación de dos factores (2FA) o se le pide «*esperar*» mientras supuestamente se verifica la información proporcionada.

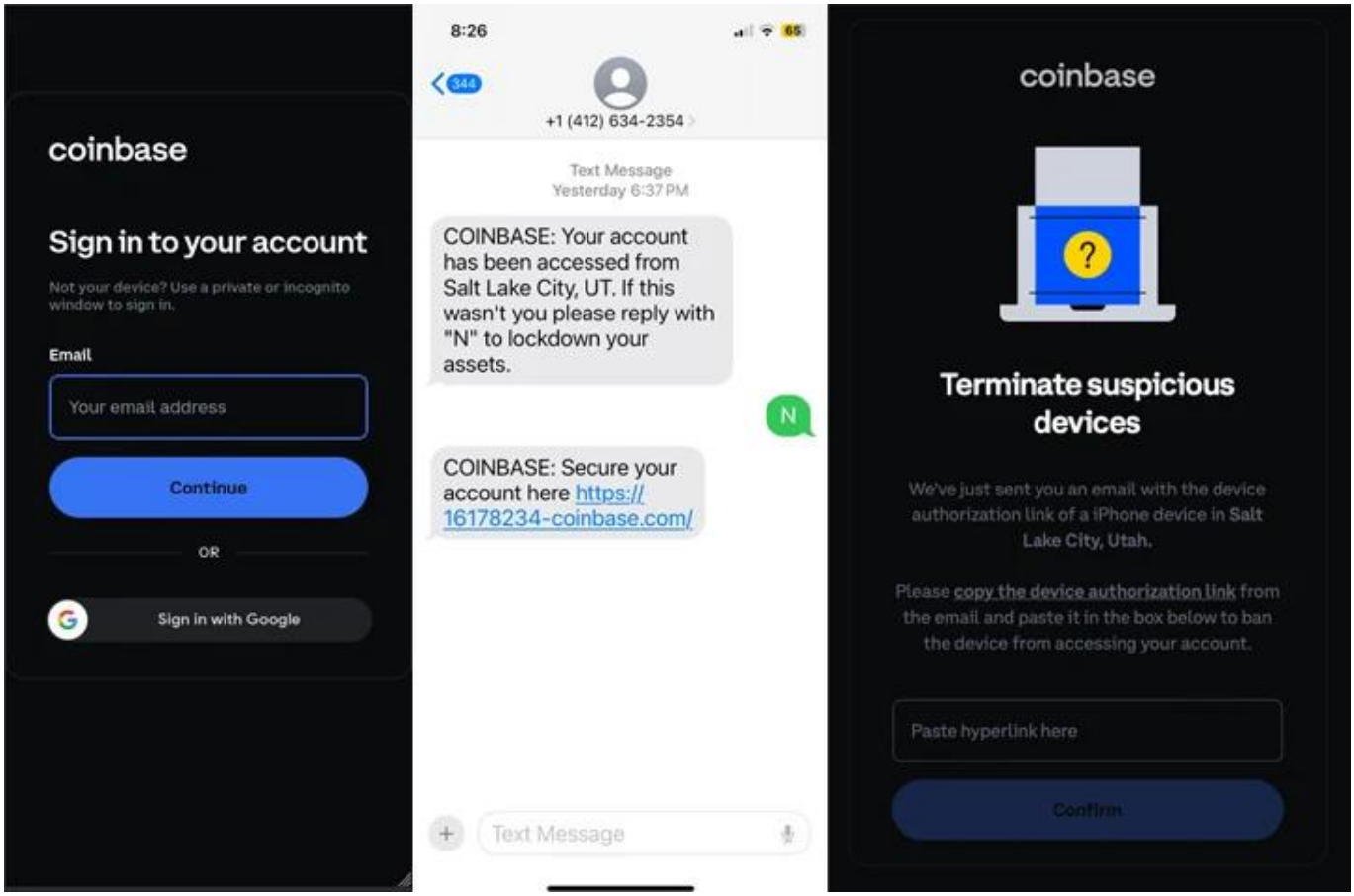
> Según Lookout, *«es probable que el atacante intente iniciar sesión en tiempo real*

> *utilizando estas credenciales y luego redirige a la víctima a la página correspondiente según la información adicional solicitada por el servicio de MFA al que el atacante intenta acceder».*

El kit de phishing también busca crear la ilusión de credibilidad al permitir que el operador personalice la página de phishing en tiempo real, proporcionando los dos últimos dígitos del número de teléfono real de la víctima y seleccionando si se debe solicitar al usuario un token de seis o siete dígitos.

El código de contraseña de un solo uso (OTP) ingresado por el usuario es capturado por el actor de amenazas, quien lo utiliza para iniciar sesión en el servicio en línea deseado utilizando el token proporcionado. En la siguiente etapa, la víctima puede ser dirigida a cualquier página elegida por el atacante, ya sea la legítima página de inicio de sesión de Okta o una página que muestre mensajes personalizados.

Lookout señala que el modus operandi de CryptoChameleon se asemeja a las técnicas utilizadas por Scattered Spider, especialmente en la suplantación de Okta y el uso de dominios previamente identificados como afiliados al grupo.



> *«A pesar de que las URL y las páginas falsificadas se asemejan a lo que Scattered Spider podría crear, hay capacidades e infraestructuras de C2 significativamente diferentes dentro del kit de phishing. Este tipo de imitación es común entre grupos de actores de amenazas, especialmente cuando una serie de tácticas y procedimientos ha tenido mucho éxito públicamente»,* indica la compañía.

Actualmente, tampoco está claro si esto es obra de un único actor de amenazas o si se trata de una herramienta común utilizada por distintos grupos.

> *«La combinación de URLs de phishing de alta calidad, páginas de inicio de sesión*

> *que se asemejan perfectamente a los sitios legítimos, un sentido de urgencia y una conexión consistente a través de SMS y llamadas de voz es lo que ha permitido a los actores de amenazas tener tanto éxito en el robo de datos de alta calidad»*, destaca Lookout.

El desarrollo de esta situación surge a medida que Fortra revela que las entidades financieras en Canadá han sido objeto de atención por parte de un nuevo grupo de phishing como servicio (PhaaS) llamado LabHost, superando en popularidad a su competidor Frappo en el año 2023.

Los ataques de phishing de LabHost se llevan a cabo a través de una herramienta de gestión de campañas en tiempo real denominada LabRat, que posibilita la ejecución de un ataque de adversario en el medio (AiTM) para capturar credenciales y códigos de autenticación de dos factores (2FA).

El actor de amenazas también ha desarrollado una herramienta de spam por mensajes de texto (SMS) llamada LabSend, que ofrece un método automatizado para enviar enlaces a las páginas de phishing de LabHost, permitiendo a sus usuarios llevar a cabo campañas de smishing a gran escala.

> *«Los servicios de LabHost permiten que los actores de amenazas apunten a diversas instituciones financieras, ofreciendo características que van desde plantillas listas para usar, herramientas de gestión de campañas en tiempo real y señuelos por SMS»,* afirmó la compañía.