GitHub publicó un aviso que detalla lo que puede ser una campaña de phishing en curso dirigida a sus usuarios por robar credenciales y códigos de autenticación de dos factores (2FA) haciéndose pasar por la plataforma CircleCI DevOps.

El servicio de alojamiento de código propiedad de Microsoft dijo que se enteró del ataque el 16 de septiembre de 2022 y agregó que la campaña afectó a *«muchas organizaciones víctimas».*

Los mensajes fraudulentos pretenden notificar a los usuarios que sus sesiones de CircleCI han expirado y que deben iniciar sesión con las credenciales de GitHub haciendo clic en un enlace.

Otro correo electrónico falso revelado por CircleCI solicita a los usuarios que inicien sesión en sus cuentas de GitHub para aceptar los nuevos Términos de uso y la Política de privacidad de la compañía siguiente el enlace incrustado en el mensaje.

Independientemente del señuelo, hacerlo redirige al objetivo a una página de inicio de sesión similar a GitHub diseñada para robar y filtrar las credenciales ingresadas, así como los códigos de contraseña de un solo uso (TOTP) en tiempo real para el atacante, lo que permite efectivamente una derivación de 2FA.

> *«Las cuentas protegidas por claves de seguridad de hardware no son vulnerables a este ataque»,* dijo Alexis Wales de GitHub.

Entre otras tácticas adoptadas por el atacante al obtener acceso no autorizado a la cuenta del usuario, se incluyen la creación de tokens de acceso personal (PAT) de GitHub, la autorización de aplicaciones OAuth o la adición de claves SSH para mantener el acceso incluso después de un cambio de contraseña.

También se ha visto al atacante descargando contenidos de repositorios privados e incluso creando y agregando nuevas cuentas de GitHub a una organización en caso de que la cuenta

comprometida tenga permisos de administración de la organización.

GitHub dijo que tomó medidas para restablecer las contraseñas y eliminar las credenciales agregadas maliciosamente para los usuarios afectados, además de notificar a los afectados y suspender las cuentas controladas por los atacantes.

La compañía insta además a las organizaciones a considerar el uso de claves de seguridad de hardware resistentes al phishing para evitar este tipo de ataques.

El último ataque de phishing se produce poco más de cinco meses después de que GitHub sufriera una campaña muy específica que resultó en el abuso de tokens de usuarios de OAuth de terceros mantenidos por Heroku y Travis CI para descargar repositorios privados.