La plataforma de alojamiento de código basada en la nube, GitHub, describió la reciente campaña de ataque que involucra el abuso de tokens de acceso OAuth emitidos a Heroku y Travis-CI como de naturaleza *«altamente dirigida».*

> *«Este patrón de comportamiento sugiere que el atacante solo estaba enumerando organizaciones para identificar cuentas a las que apuntar selectivamente para enumerar y descargar repositorios privados»,* dijo Mike Hanley, de GitHub.

El incidente de seguridad, que se descubrió el 12 de abril, estaba relacionado con un atacante no identificado que aprovechaba los tokens de usuario de OAuth robados emitidos a dos integradores de OAuth de terceros, Heroku y Travis-CI, para descargar datos de docenas de organizaciones, incluyendo NPM.

La compañía propiedad de Microsoft dijo la semana pasada que está en el proceso de enviar un conjunto final de notificaciones a los clientes de GitHub que tenían las integraciones de la aplicación Heroku o Travis CI OAuth autorizadas en sus cuentas.

Según un análisis detallado paso a paso realizado por GitHub, se dice que el adversario empleó los tokens de la aplicación robados para autenticarse en la API de GitHub, usándolos para enumerar todas las organizaciones de los usuarios afectados.

Esto se logró eligiendo objetivos de forma selectiva en función de las organizaciones enumeradas, siguiendo enumerando los repositorios privados de cuentas de usuarios valiosos, antes de pasar finalmente a clonar algunos de esos repositorios privados.

La compañía también reiteró que los tokens no se obtuvieron por medio de un compromiso de GitHub o sus sistemas, y que los tokens no se almacenan en sus *«formatos originales y reutilizables»,* que podrían ser mal utilizados por un atacante.

> *«Los clientes también deben continuar monitoreando a Heroku y Travis CI para*

> *obtener actualizaciones sobre sus propias investigaciones sobre las aplicaciones OAuth afectadas»,* dijo GitHub.