Investigadores de seguridad cibernética descubrieron una lista de 3207 aplicaciones, algunas de las cuales pueden usarse para obtener acceso no autorizado a cuentas de Twitter.

La adquisición es posible debido a una filtración de información legítima de Consumer Key y Consumer Secret, dijo la compañía de seguridad cibernética CloudSEK con sede en Singapur.

> *«De 3,207 aplicaciones, 230 están filtrando la cuatro credenciales de autenticación y se pueden usar para hacerse cargo por completo de sus cuentas de Twitter y pueden realizar cualquier acción crítica/sensible»,* dijeron los investigadores.

Esto puede variar desde leer mensajes directos hasta realizar acciones arbitrarias como retuitear, dar me gusta y eliminar tuits, seguir cualquier cuenta, eliminar seguidores, acceder a la configuración de la cuenta e incluso, cambiar la imagen de perfil de la cuenta.

El acceso a la API de Twitter requiere generar las Claves y los Tokens de acceso, que actúan como los nombres de usuario y las contraseñas de las aplicaciones, así como de los usuarios en cuyo nombre se realizarán las solicitudes de la API.

Un atacante en posesión de esta información puede, por lo tanto, crear un ejército de bots de Twitter que podría aprovecharse potencialmente para difundir información errónea/desinformación en la plataforma de redes sociales.

> *«Cuando se pueden utilizar múltiples adquisiciones de cuentas para cantar la misma melodía en tándem, solo se retira el mensaje que debe distribuirse»,* agregaron los investigadores.

Además, en un escenario hipotético explicado por CloudSEK, las claves API y los tokens recopilados de las aplicaciones móviles se pueden integrar en un programa para ejecutar campañas de malware a gran escala por medio de cuentas verificadas para dirigirse a los

seguidores.

Además de la preocupación, debe tenerse en cuenta que la filtración de claves no se limita solo a las API de Twitter. En el pasado, los investigadores de CloudSEK descubrieron las claves secretas de las cuentas de GitHUB, AWS, HubSpot y Razorpay de aplicaciones móviles desprotegidas.

Para mitigar este tipo de ataques, se recomienda revisar el código de las claves de API directamente codificadas, al mismo tiempo que rotar periódicamente las claves para ayudar a reducir los riesgos probables derivados de una fuga.

> *«Las variables en un entorno son medios alternativos para referirse a las claves y disfrazarlas además de no incrustarlas en el archivo fuente»,* dijeron los investigadores.

> *«Las variables ahorran tiempo y aumentan la seguridad. Se debe tener cuidado adecuado para garantizar que no se incluyan archivos que contengan variables de entorno en el código fuente».*