Herramienta Que Te Permite Hackear Cuenta En iCloud

El hacker apodado «Pr0x13» ha lanzado una **herramienta de hacking** para contraseñas de las cuentas en iCloud en la ***página web de GitHub,*** asegura que los atacantes pueden **vulnerar cualquier cuenta de iCloud**, lo que potencialmente les da libre acceso a los dispositivos iOS de las víctimas.

La herramienta se llama **iDict**, en realidad hace **uso de una vulnerabilidad** en la infraestructura de seguridad de iCloud de Apple para eludir restricciones de seguridad y autenticación de dos factores que impide ataques de fuerza bruta y mantiene la mayoría de los hackers lejos del acceso a las ***cuentas de los usuarios de iCloud***.

Como podrás recordar, este fallo de seguridad en iCloud, permitió la intrusión a una variedad de cuentas de famosos, de las cuales se pudieron extraer fotos intimas de ellos. ***Pr0x13*** afirma que iDict puede ser «100 por ciento», eficaz y fácil de usar para el inicio de sesión en cuenta individuales. Por lo tanto, aquellos que utilizan contraseñas fáciles de adivinar en su cuenta de iCloud están en potencial peligro en comparación de los que utilizan una cadena compleja.

A pesar de innumerables advertencias y consejos en el pasado, los usuarios en línea están constantemente utilizando una fuerza débil en las cadenas de contraseñas como «password», «12345678», «qwerty,» «abc123» y «iloveyou», esperando que esta «seguridad» sea lo suficiente para proteger los datos mas sensibles, sin duda, ahora tienes de que preocuparte.

Actualmente iDict se encuentra ***alojado en GitHub***, y está limitada por el tamaño del diccionario que usa la herramienta para adivinar la contraseña. En ese momento, el archivo de diccionario sólo contiene 500 palabras en la lista

de contraseñas. Esto significa que tendras exito al 100% si intentas 500 veces. Sin embargo, un atacante con una lista de mayor tamaño, puede ser capaz de comprometer más cuentas, sin embargo, esperamos que Apple pueda solucionar este problema antes de que suceda algun hackeo.

Pr0x13 comenta que sus intenciones son sólo para **alertar de Apple acerca de la vulnerabilidad**, por lo que la compañía podría solucionar el problema lo antes posible. La herramienta, de acuerdo con el hacker, ha sido puesto en libertad para forzar a Apple a actuar en el tema y nada más. La empresa tiene que solucionar la vulnerabilidad antes de que sea usada para extraer datos importante, explica Pro0x13 en GitHub.

Apple tiene que actuar con rapidez en el tema para evitar otro escándalo polémico por robo de fotos. Como precaución, asegúrese de que la contraseña no aparece en el archivo de contraseñas de ***Pr0x13*** y si es así, debes cambiarla inmediatamente. También cambia la contraseña si utiliza una contraseña débil! Además, **habilite la autenticación de dos factores en todas sus cuentas**, si no lo ha hecho.