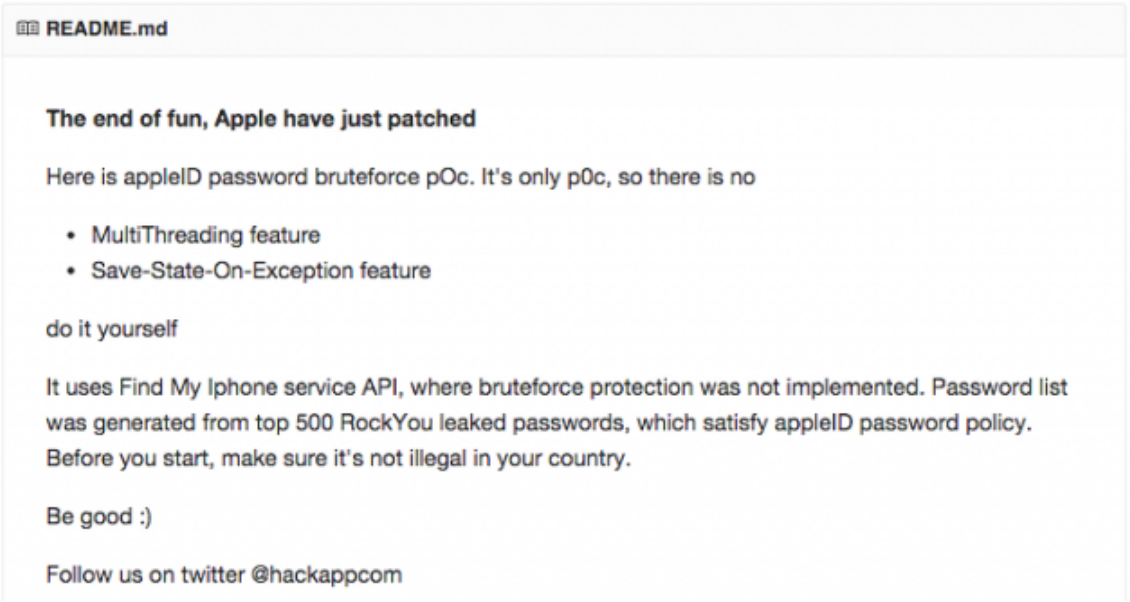
# El Script Que Permitió El Acceso A iCloud

Un **script en Python** seria la herramienta que habría permitido el **acceso a iCloud** por parte de «Hackers» quienes ha tenido acceso a ciertas fotos intimas de algunas personas famosas de Hollywood. Este script surgió en GitHub, el cual parece haber permitido a algunos usuarios maliciosos usar el método de «fuerza bruta» para obtener la contraseña de las cuentas que usan iCloud, esto se debe a una vulnerabilidad en el servicio **Find My iPhone**. Los ataques de fuerza bruta consisten en utilizar un **script malicioso** para adivinar repetidamente hasta encontrar la contraseña correcta.


README.md

**The end of fun, Apple have just patched**

Here is appleID password bruteforce pOc. It's only p0c, so there is no

- MultiThreading feature
- Save-State-On-Exception feature

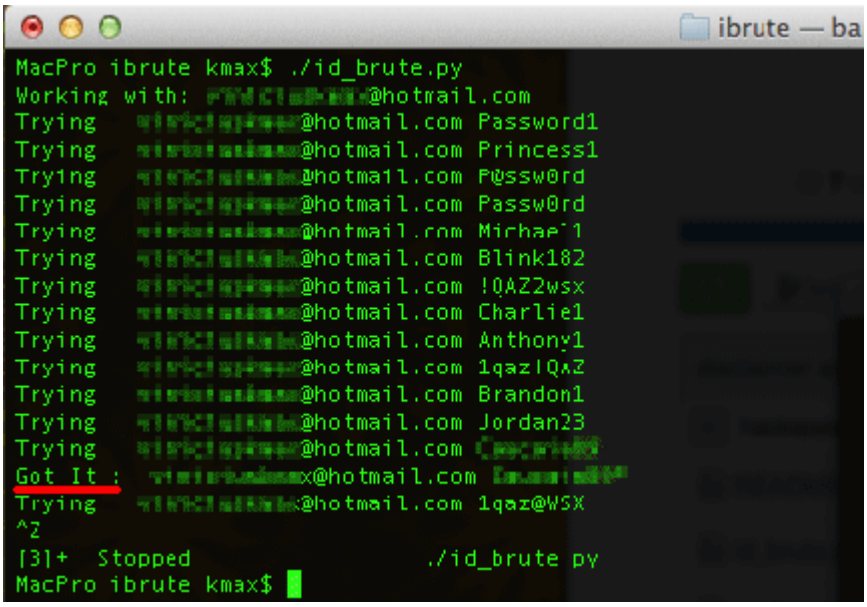
do it yourself

It uses Find My Iphone service API, where bruteforce protection was not implemented. Password list was generated from top 500 RockYou leaked passwords, which satisfy appleID password policy. Before you start, make sure it's not illegal in your country.

Be good :)

Follow us on twitter @hackappcom

La **vulnerabilidad en el servicio Find My iPhone** parece haber dejar que los atacantes utilizan este método para adivinar las contraseñas en varias ocasiones sin ningún tipo de bloqueo ó de alerta a los usuarios del servicio. Una vez que la contraseña ha sido finalmente encontrada, el atacante puede este ingreso para acceder a otras **funciones de iCloud** como si se tratase del usuario original.




Los **usuarios de Twitter** fueron capaces de utilizar la herramienta de GitHub, el cual se publicó durante dos días antes de ser compartida por Hacker News, la cual fue usada para acceder a sus propias cuentas, al parecer Apple ya ha parcheado este **problema de seguridad**. El propietario de la herramienta se dio cuenta de que fue parcheado a las 3:20 am PT.

Algunos usuario han probado la herramienta, despues de cinco intentos se han bloqueado las cuentas, lo que significa que el script de Python sin duda trata de atacar el servicio, pero Apple ha eliminado este agujero :(

Según comento el creador de la herramienta maliciosa, Hackapp, en Twitter, «este error es común para todos los servicios que tienen muchas interfaces de autenticación», y que con «el conocimiento básico de rastreo de datos y las técnicas de reversión» es «trivial» para descubrir los **datos mas sensibles**. Con esto podemos saber que cualquier puede hacer uso de esta herramienta y tratar de sacar la información de cualquier persona que use el servicio vulnerado, aunque haya sido solucionado, existirán otros servicios que tengan el mismo problema de seguridad.

**Hackapp** también publicó una presentación que detalla la

herramienta, por lo que fue creado e identifica otros problemas en la seguridad del **llavero de claves de iCloud**. En vista de la «gravedad» que presenta el uso de esta herramienta, la presentación ha sido eliminada del servicio web que la alojaba.

Aun no está claro cuánto tiempo ha estado abierto este grave agujero de seguridad, dejando vulnerables a los usuarios de este servicio, los atacantes solo necesitaban una dirección de correo electrónico y algo de paciencia para encontrar la clave correcta para ingresar a la cuenta del afectado. Todavía no existe evidencia precisa de que estas imágenes se han filtrado a través de iCloud y pudieron haber sido obtenidas mediante el ataque a otros servicios. Aunque la persona que ha filtrado estas imágenes, aseguro que se han obtenido por medio de iCloud.

¿Están seguros tus datos?