Instasheep: secuestrar cuentas de Instagram en una red Wi-Fi

Publicado por Vicente Motos on martes, 29 de julio de 2014 Etiquetas: herramientas , noticias , técnicas , vulnerabilidades

Stevie Graham, un programador de Londres, presentó recientemente un informe a Facebook describiendo lo que él veía como una vulnerabilidad en Instagram que podía permitir a alguien secuestrar la sesión de un usuario en base a los datos capturados a través de una red Wi-Fi pública.

Cuando Facebook le dijo que no iba a obtener una recompensa por el bug, Stevie se dedicó a preparar una herramienta de prueba de concepto para explotarla. "*Denegado el programa de recompensas. El siguiente paso es escribir una herramienta automatizada que permite el secuestro masivo de cuentas*", escribió. "*Vuln bastante grave, FB. por favor arreglarla*".

Instagram utiliza HTTP para gran parte de sus comunicaciones, transmitiendo en claro el nombre de cuenta del usuario y el id. Y como Graham demostró, hay otros datos que se envían entre el cliente iOS de Instagram y el servicio que se pasan en claro.
A pesar de que las credenciales del usuario se envían utilizando una conexión segura, la información pasa de nuevo por la interfaz de la aplicación de Instagram al teléfono y proporciona una cookie que se puede utilizar en la misma red sin reautenticación para conectar a través de la Web a Instagram como ese usuario y tener acceso a mensajes y otros datos. "*Una vez que tenga una cookie, cualquier punto final puede ser autenticado con la cookie, HTTPS o HTTP*", comentó. Stevie dijo también que él conocía este fallo durante años.

Graham ha publicado los siguientes pasos para reproducir el exploit:

- conecta con un punto de acceso abierto o WEP
- pon el interfaz en modo promiscuo y filtra i.instagram.com: `sudo tcpdump -In`

```
-i en0 -s 2048 -A dst i.instagram.com
```
- espera a que alguien con iOS use Instagram
- extrae la cookie de la cabecera de la petición del resultado de la salida
- utiliza el parámetro de la cookie sessionid para cualquier llamada al api (incluido https y mensajes directos):

```
  curl -H 'User-Agent: Instagram 6.0.4 (iPhone6,2; iPhone OS 7_1_1;
en_GB; en-GB) AppleWebKit/420+' \ -H 'Cookie: sessionid=REDACTED' \
https://i.instagram.com/api/v1/direct_share/inbox/`
```

Esto nos llevará a la bandeja de entrada de mensajes directos del usuario como JSON (JavaScript Object Notation).

Como veis este tipo de exploit es similar a "Firesheep" y por eso Stevie llamó a su herramienta "Instasheep". Aunque de momento seguimos esperando su código en su repositorio: https://github.com/stevegraham/instasheep.

Fuentes:
- Instasheep: Coder builds tool to hijack Instagram accounts over Wi-Fi
- Using Instagram on public Wi-Fi risks account hijack