Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Motorola Is Listening : Motorola os espía y roba vuestros passwords (4008 lectures)

Per **René Mérou**, ***H*** (http://h.says.it/)

Creado el 02/07/2013 05:37 modificado el 21/07/2013 21:36

> El enlace es dinamita pero como lo prometido es deuda aquí os pongo traducido una parte.
>
> Haciendo un resumen de la situación creo que podemos decir que nuestras democracias está siendo destruidas atacando sus fundamentos. Los derechos fundamentales de todas las constituciones, empezando por el derecho a la privacidad. No hay que olvidar que es precisamente la privacidad lo que más estorba a los gobiernos dictatoriales a la hora de perseguir a los opositores.
>
> Enrique Dans describe un poco más lo que pasa en su artículo Agotando toda capacidad de sorpresa[1].

El enlace: Motorola Is Listening[2] artículo en inglés de Ben Lincoln[3]

Esto y el asunto del espionaje del FBI/CIA/NSA revelado hace poco usando Google, Facebook y otras corporaciones que llega desde políticos a quienes hay que corromper/presionar/liar/engañar/puentear hasta a los simples usuarios de la calle con poder o nivel de riquezas infimos...

Ben Lincoln ha ido ampliando el artículo dado el éxito que tiene y otras cosas que ha ido encontrando. Para los que no están muy puestos en inglés aquí van algunas partes traducidas.

Descubrimiento

Estaba usando mi teléfono personal en el trabajo para hacer algunos tests relacionados con Microsoft Exchange ActiveSync. Para monitorizar el trafico, configuré mi teléfono para usar un proxy con todo el trafico http y https a través de Burp Suite Professioal- un proxy para interceptar que solemos usar para tests de penetración - de forma que podría fácilmente ver los contenidos de la comunicación ActiveSync.

Mirando a través del historial del proxi veo frecuentemente conexiones http hacia ws-cloud112-blur.svcmot.com mezcladas en las conexiones ActiveSync.

Como el 22 de Junio del 2013, svcmot.com que es un dominio de Motorola.

Fui rápidamente capaz de determinar que las conexiones hacia Motorola se provocaban cada vez que actualizaba la configuración del ActiveSync en mi móvil, y el tráfico no cifrado http contenía los siguientes datos:

1- El nombre del DNS del servidor ActiveSync (sólo cuando la configuración es creada por primera vez).
2- El nombre de dominio y el identificador del usuario que yo ponía para la autenticación.
3- El email completo de la cuenta.
4- El nombre de la conexión.

A medida que miraba en el historial del proxi pude ver conexiones menos frecuentes en las cuales se enviaban fragmentos de datos mayores - por ejemplo, una lista de todos los atajos de aplicaciones y widgets presentes en mi pantalla principal.

Análisis - email, ActiveSync, y redes sociales

Decidí probar a configurar cada una de los otros tipos de cuentas que el systema me dejaba y averiguar que se capturaba.

Facebook y twitter

Para ambos servicios, el email y el password de la cuenta eran enviados a Motorola. Ambos servicios soportan un mecanismo (oAuth) explícitamente diseñado para hacer esto innecesario, pero Motorola no usa ese más seguro mecanismo. El password es solo enviado en https, por lo que al menos no puede ser interceptado por la mayoría de terceras partes.

La mayoría de las subsecuentes conexiones de ambos servicios (que no sean bajar imágenes) se envían a través del proxi del sistema de Motorola usando http, de forma que morotorla y cualquiera ejecutando una captura en la red puede ver cuales son tus amigos o contactos y (incluyendo sus emails), que publicas y lees, y más cosas del estilo. Ellos también obtienen una lista de las imágenes que estas viendo, incluso cuando la descarga de la imágen es directa de la fuente.

En la imagenes se ve que se puede ver el password y el usuario en facebook entre otras redes. Un montón de imágenes impresionantes de capturas.

Se habla de Picasa, Photobucket, youtube, yahoo, flickr, gmail, firefox.

Realmente vale la pena leerlo entero en inglés enlaces incluidos. :)

Lista de enlaces de este artículo:

1. http://www.enriquedans.com/2013/08/agotando-toda-capacidad-de-sorpresa.html
2. http://www.beneaththewaves.net/Projects/Motorola_Is_Listening.html
3. http://www.beneaththewaves.net/About/Ben_Lincoln.html

E-mail del autor: ochominutosdearco _ARROBA_ gmail.com