Tapa tu CAM ante miradas indiscretas

04/09/2015

Espiar a través de la cámara Web puede ser más fácil de lo que parece, con ciertos conocimientos informáticos y software disponible por la red se puede realizar esta actividad tan poco ética y deleznable si se realiza sin el consentimiento de los que están siendo vistos.

Existe una categoría de software de administración remota (RAT) con el que básicamente se puede tener **control del ordenador** remoto así como de sus periféricos. Muchos de los troyanos más famosos están basados en este tipo de software con el que se pueden hacer fotografías desde tu webcam, grabar sonidos con tu micrófono e incluso formatear el disco duro, aparte de poder ver vídeo en directo.

El tema es más peliagudo de lo que pueda parecer. Al final del 2014 una Web rusa decidió mostrar en tiempo real miles cámaras de todo el mundo sin que sus protagonistas fueran conscientes de ello. Se contabilizaron **más de 400 cámaras situadas en España** donde se podía ver a los protagonistas trabajando en su oficina, en el salón de su casa o mientras hacían la cena. Este caso llamó aún más la atención porque no se detectó software espía sino que los equipos no habían cambiado las credenciales de fábrica con las que los atacantes consiguieron tomar el control.

Un caso anterior a finales de 2013 fue el de la Miss adolescente de EEUU Cassidy Wolf, Cassidy solía dejar la pantalla de su MacBook abierta en el salón de su casa sin

ser consciente de que alguien había estado activando y grabando con su Webcam. Un día al llegar a casa y descargar el correo empezó a leer hasta llegar a uno que le llamó la atención de un remitente anónimo que le adjuntaba un par de imágenes. Al abrirlas, Cassidy no podía creer lo que estaba viendo: era ella misma en su apartamento en diferentes momentos.

En este caso se trataba de un acosador que estuvo chantajeándola pidiendo vídeos y fotos posando desnuda. Tras unos días sin poder dormir la Miss tomó la vía más sensata y denunció el caso ante el FBI.
La evolución de este software está en aumento, incluso sus autores están haciendo negocio con ello ya que cada vez son más fáciles de utilizar por alguien mal intencionado, y no me cabe la menor duda de que el próximo objetivo son los teléfonos inteligentes, intentaré hablar de esto en un futuro artículo, software de control de dispositivos móviles y los buenos y malos usos que se les puede dar.

¿Y cómo se puede evitar todo esto? No es una pregunta fácil de responder ya que las formas de hackear son diversas, pero sí se me ocurre dar unas pautas básicas.

- **Actualiza tu sistema operativo** periódicamente a la última versión.
- Cuidado por los sitios donde navegas y que descargas en tu equipo.
- Y lo más evidente y práctico, **tapa la cámara de tu portátil cuando no la estés utilizando**, puede ser con un simple papel y celo o utilizando algún tipo de tapa como las que tienen en www.tapatucam.com (de Málaga) y tienen unas tapas muy graciosas que puedes comprar en su propia Web.