Publicado en el 04/11/2016

El nuevo objetivo de los hackers son las bombillas "inteligentes"

Las llamas bombillas "inteligentes" como las Philips Hue ya han sido blancos de hackeo en el pasado, donde a pesar de que se necesita estar ante una situación bastante complicada, la vulnerabilidad está ahí.

Se sabía que llegaría este día, el que pondría en evidencia la inseguridad que existe en muchos de los dispositivos del Internet de las Cosas o IoT, que como se pudo saber hace unos días, los protagonistas de un gran ataque DDoS, donde un ejercito de cámaras IP y dispositivos grabadores fueron los responsables de que algunos de los servicios más populares de internet dejarán de funcionar por unas horas.

Las llamas bombillas "inteligentes" como las Philips Hue ya han sido blancos de hackeo en el pasado, donde a pesar de que se necesita estar ante una situación bastante complicada, la vulnerabilidad está ahí. En esta ocasión se verá cómo un grupo de hackers, de los llamados white-hat, muestran una nueva vulnerabilidad que no tiene nada que ver con lo mostrado en el pasado, ya que para tomar el control del dispositivo se necesita un drone.

Sólo se necesita un drone y un firmware malicioso

Debido a los hackeos que han sufrido las bombillas "inteligentes", Phillips ha actualizado la seguridad para que este trabajo sea más complicado, además de que es necesario estar ante un escenario donde el atacante necesita estar en la misma red que las bombillas y tener control de un ordenador local, lo que lo vuelve una tarea compleja y casi imposible.

Pero ahora esta nueva vulnerabilidad no requiere ese tipo de acceso, ya que sólo se necesita engañar a las bombillas para que acepten una actualización de software vía WiFi que explota una debilidad incluida en el sistema Touchlink del sistema ZigBee Light Link, el mismo que ha sido atacado en varios otros dispositivos.

Para instalar este firmware sólo se necesita un drone o un vehículo que pase a menos de 70 metros de donde están las bombillas, donde una vez instalado será posible extraer la clave global AES-CCM del fabricante, lo que permitirá desactivar cualquier nueva actualización y así tomar control total del dispositivo. Pero lo más interesante es que sólo se necesita infectar una bombilla, ya que será ésta la que se encargue de esparcir el firmware entre toda la red y así en máximo 10 minutos hacerse con el control.

Estos hackers pertenecen al Instituto Weizmann de Ciencias y la Universidad de Dalhousie, y su objetivo es mostrar los detalles de la vulnerabilidad para que el fabricante responsable lo arregle cuanto antes. Por lo anterior han publicado todos los detalles de este trabajo.

La noticia El nuevo objetivo de los hackers son las bombillas "inteligentes" fue publicada originalmente en Xataka

Datos de contacto:

Nota de prensa publicada en:

Categorías: Telecomunicaciones Hardware E-Commerce Software