Publicado en México el 06/10/2017

# [Avast comprueba la seguridad de dispositivos conectados a internet](http://www.notasdeprensa.es)

## El Laboratorio de Amenazas de Avast, líder en productos de seguridad digital, comprueba la seguridad de los dispositivos conectados a internet y cómo pueden hackearse para ofrecer recomendaciones de seguridad

 Avast dio a conocer algunos tips de seguridad de cómo pueden hackearse algunos dispositivos inteligentes también conocidos como IoT o ` Internet de las Cosas´ como juguetes, muebles, coches, dispositivos médicos, hasta botellas de agua que ya empiezan a fabricarse. Por qué no son seguros los dispositivos inteligentesLos fabricantes se ven presionados para producir dispositivos inteligentes y lanzarlos al mercado rápidamente a un precio accesible. Esto hace que a menudo, se descuide la seguridad. Por ejemplo, un fabricante que ahora se dedique a producir tostadoras inteligentes nunca ha tenido la necesidad de proteger sus tostadoras tradicionales de los hackers. Este es uno de los motivos por los que la seguridad de estos dispositivos es escasa o insuficiente. Es más, no existen requisitos en el sector que los fabricantes deban cumplir en relación con la seguridad, por lo que deben crear sus propios estándares de comunicación, y estos no siempre contemplan la seguridad como algo prioritario. Esto significa que se lanzan al mercado dispositivos inteligentes sin estándares básicos de seguridad adaptados a los tiempos actuales. ¿Se pueden hackear los dispositivos inteligentes?Dado que estos dispositivos están desprotegidos, se pueden hackear de muchas maneras. Puede ser tan fácil como obtener las credenciales de acceso mediante un ataque de fuerza bruta, o bien hacerse de forma más sofisticada: con diversas técnicas para aprovechar vulnerabilidades o recreando firmware o sistemas operativos para encontrar vulnerabilidades de día 0. En la darknet se ofrecen servicios y códigos exploit para hackear dispositivos conectados a Internet, por lo que son cada vez más los usuarios que pueden acceder a ellos. Los hackers siempre intentan infiltrarse en nuevos tipos de red y en los sistemas de comunicación que emplean estos dispositivos. ¿Es difícil hackear un dispositivo conectado a Internet?El modo más sencillo de hackear un dispositivo inteligente es mediante un ataque de fuerza bruta para descifrar contraseñas o intentar acceder con las credenciales de acceso predeterminadas del dispositivo. Cualquier hacker aficionado puede alquilar una botnet en la darknet e infectar miles de dispositivos de una vez. Muchos fabricantes utilizan las mismas credenciales de acceso predeterminadas en todos sus dispositivos para ahorrar costos en lugar de crear una contraseña exclusiva para cada uno. La botnet Mirai fue una de las mayores amenazas del año pasado en el Internet de las cosas, ya que infectó miles de dispositivos inteligentes utilizando credenciales de acceso predeterminadas para perpetrar ataques DDoS masivos. Dado que el código fuente de Mirai se hizo público, cualquiera podía ejecutar la botnet o modificar su código, por lo que se crearon muchas mutaciones de ésta. También hay otras formas más complejas y caras de infectar un dispositivo inteligente y, por lo tanto, menos comunes. Por ejemplo, recrear firmware o un sistema operativo requiere conocimientos técnicos avanzados y, además, lleva tiempo. Por otra parte, un código exploit que aproveche una vulnerabilidad de día 0 puede costar miles de dólares. Medidas necesarias para mejorar la seguridad de los dispositivos inteligentesUn modo eficaz de mejorar drásticamente la seguridad de los dispositivos inteligentes es facilitarle al usuario el cambio de las credenciales de acceso. Para ello, el fabricante puede, por ejemplo, imponer como requisito la creación de una contraseña única y segura a la hora de configurar el dispositivo por primera vez. Por supuesto, esto no es posible en todos los casos, pero basta con cambiar las credenciales de acceso predeterminadas para reducir en gran medida la cantidad de dispositivos desprotegidos y hacer más difícil que un hacker novato o aficionado o un robot de búsqueda simple accedan a estos dispositivos. El fabricante también puede incluir en cada dispositivo una contraseña única y aleatoria. Por otra parte, lanzar actualizaciones de software que corrijan vulnerabilidades contribuiría a proteger los dispositivos inteligentes de códigos exploit. Actualmente, los fabricantes suelen utilizar versiones desactualizadas de varias bibliotecas y sistemas operativos para los que existe un gran número de exploits potentes, dejando expuesto el dispositivo a los ataques. En muchos dispositivos, no es posible actualizar el firmware. Si, en estos casos, un hacker lograra aprovechar una vulnerabilidad, la única solución sería, básicamente, desconectar el dispositivo de la red de forma permanente y sustituirlo por otro más seguro. Mejorar la seguridad de los dispositivos inteligentes no solo permitiría proteger la privacidad del usuario y evitar ataques DDoS, sino también prevenir consecuencias mucho peores. Se han realizado ataques de prueba con los que se han infectado redes enteras de dispositivos a través de un solo dispositivo, como puede ser una bombilla o un sensor de tráfico. Esto demuestra el gran problema que representa un dispositivo inteligente con vulnerabilidades y el daño que puede causar si cae en manos malintencionadas. Imagine si un hacker llegara a controlar el tráfico o apagar todas las luces de una ciudad. Los fabricantes de dispositivos inteligentes deberían colaborar con expertos en seguridad para implantar una capa de protección en los dispositivos y realizar pruebas de infiltración con regularidad.

**Datos de contacto:**

Flor Carreno

Marketing Q S SA de CV

56152198

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-comprueba-la-seguridad-de-dispositivos\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Nacional E-Commerce Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)