OVATION AMERICAS

Boletín Abril 2022

¿Tus dispositivos te están espiando? (Parte 1)

Cada vez más objetos y dispositivos en el hogar están conectados a Internet, lo que los hace potencialmente en riesgo de ser pirateados.

Desde televisores conectados a Internet, juguetes, refrigeradores, hornos, cámaras de seguridad, cerraduras de puertas, rastreadores de ejercicios y luces, el llamado "Internet de las cosas" (IoT) promete revolucionar nuestros hogares.

Pero también amenaza con aumentar nuestra vulnerabilidad a actos maliciosos. Las brechas de seguridad en dispositivos IoT son comunes. Los hackers pueden explotar estas vulnerabilidades para tomar el control de los dispositivos, robar o modificar datos y espiarnos.

En reconocimiento de estos riesgos, muchos gobiernos han introducido un nuevo código de prácticas para alentar a los fabricantes a hacer que los dispositivos IoT sean más seguros. El código proporciona orientación sobre contraseñas seguras, la necesidad de parches de seguridad, la protección y eliminación de los datos personales de los consumidores y la notificación de vulnerabilidades, entre otras cosas.

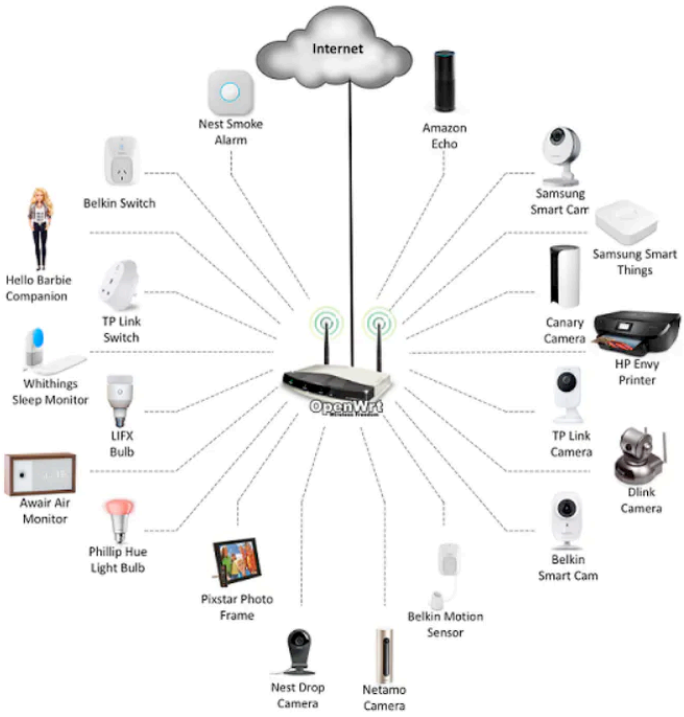
El problema es que la mayoría de las veces, el código es voluntario. Otras experiencias, como en el Reino Unido, sugieren que un código voluntario será insuficiente para proporcionar las protecciones que los consumidores necesitan. De hecho, incluso podría aumentar los riesgos, al arrojar a los consumidores a una falsa sensación de seguridad sobre la seguridad de los dispositivos que compran.

Muchos dispositivos IoT no son seguros

Los dispositivos IoT diseñados para consumidores son generalmente menos seguros que las computadoras convencionales.

En 2017, la Red Australiana de Acción del Consumidor de Comunicaciones encargó a investigadores de la Universidad de Nueva Gales del Sur que probaran la seguridad de 20 electrodomésticos que se pueden conectar y controlar a través de Wi-Fi.

Estos incluían un televisor inteligente, un altavoz portátil, un asistente de voz, una impresora, un monitor de sueño, un marco de fotos digital, básculas de baño, una bombilla, un interruptor de encendido, un detector de humo y una muñeca parlante Hello Barbie.



Si bien algunos dispositivos (incluida la Barbie) demostraron ser relativamente seguros en términos de privacidad, todos tenían algún tipo de falla de seguridad.

Muchos "han permitido violaciones potencialmente graves de la seguridad y la protección".

Lo que esto podría significar potencialmente es que alguien podría, por ejemplo, piratear la red Wi-Fi de un hogar y recopilar datos de dispositivos IoT.

Esto puede ser tan simple como saber cuándo están encendidas las luces para determinar cuándo se puede irrumpir en una casa.

Alguien con intenciones más maliciosas podría encender su horno mientras apaga los detectores de humo y otros sensores.

Riesgos para los consumidores y la sociedad.

Los factores que conducen a una seguridad deficiente en los dispositivos IoT incluyen el deseo de los fabricantes de minimizar los componentes y reducir los costos.

Muchos fabricantes de bienes de consumo también tienen poca experiencia con problemas de ciberseguridad. Combinado con el hecho de que muchos consumidores no son lo suficientemente expertos en tecnología como para apreciar los riesgos y protegerse, esto crea la posibilidad de explotar los dispositivos IoT.

A nivel personal, podrías ser espiado y acosado. Las fotos o la información personal podrían estar expuestas al mundo o utilizadas para extorsionarlo.

A nivel social, los dispositivos IoT pueden ser secuestrados y utilizados colectivamente para cerrar servicios y redes. Incluso comprometer un dispositivo puede hackear la infraestructura conectada.

Esta es una preocupación creciente a medida que más y más personas se conectan a las

redes de trabajo desde casa. Estos nuevos dispositivos IoT a menudo nos hacen la vida más fácil. Los dispositivos IoT pueden mejorar la eficiencia, la conveniencia, la productividad o la calidad general de nuestras vidas.

Pero, siempre hay una compensación entre su valor para mejorar la vida y una posible pérdida de privacidad. Muchos de los prácticos dispositivos IoT que usamos en casa, en el trabajo, en el automóvil o donde quiera que vayamos **también plantean riesgos de espionaje**. Este es el caso de tres dispositivos IoT recientemente introducidos.

Apple Air Tags

Un dispositivo IoT que proporciona una manera fácil de rastrear sus objetos. (por ejemplo, billetera, llaves, bicicleta, etc.)

Funciones:

- Se conecta a tu dispositivo Apple para ayudarte a localizar los elementos que has etiquetado con el AirTag de Apple
- Actúa como una baliza emitiendo un sonido para que pueda localizar sus objetos etiquetados
- Envía una señal Bluetooth detectada por dispositivos cercanos en la red Localizar y envía la ubicación del AirTag a iCloud

- Utiliza la red Find My (con más de 100 millones de dispositivos iPhone, iPad y Mac en todo el mundo) para ayudarlo a localizar sus artículos etiquetados.
- Usa Precision Finding con un Apple iPhone 11 o posterior junto con la aplicación Buscar mi y Siri para encontrar tus artículos etiquetados.

Riesgos:

1. Un espía puede conectar un AirTag a su dispositivo Apple y luego dejar caer el AirTag en su bolsillo, bolso, mochila, automóvil, etc. Pueden rastrear su paradero al alcance de la etiqueta en una ventana de 8-24 horas usando su iPhone. El espía puede capturar su ubicación, movimientos, dirección de residencia y lugares visitados con frecuencia.

2. El AirTag se puede abrir y reprogramar con fines maliciosos. Sí, los investigadores de seguridad hackearon el AirTag en menos de 10 días.
3. Si está utilizando un dispositivo Android, la única forma de saber si hay un AirTag cerca es el sonido emitido por el AirTag de Apple. El sonido comienza después de un período de inactividad (rango de 8 a 24 horas). Pero, si no puede escuchar el sonido emitido por el AirTag y no usa un iPhone, el espía puede continuar rastreándolo durante aproximadamente un año, que es aproximadamente la duración de la batería. ¡Una aplicación Tracker Detect para Android ya está disponible en Apple!

Amazon Sidewalk

Un dispositivo IoT que crea una red de "malla" compartida de dispositivos interconectados.

Funciones:

- Crea una red de bajo ancho de banda utilizando dispositivos Sidewalk Bridge .
. Comparte parte de su ancho de banda de Internet con un grupo que proporciona servicios a usted / sus vecinos (ancho de banda máximo 80Kbps, 500 MB por mes por límite de cliente).
- Proporcionado por Amazon sin costo para los clientes
- Simplifica la configuración de nuevos dispositivos
- Amplía el rango de trabajo de bajo ancho de banda de dispositivos como rastreadores (por ejemplo, Tile)
- Puede ayudar a los dispositivos a mantenerse en línea incluso cuando están fuera del alcance de la red Wi-Fi de su hogar.

Riesgos:

1. Un espía/hacker se conecta a la red de Amazon Sidewalk, utiliza malware para penetrar en los dispositivos y realiza actividades ilegales con su dispositivo.

2. La red de un vecino no está protegida correctamente, pero está conectada a Amazon Sidewalk. Un hacker coloca ransomware en la red / dispositivos del vecino y el ransomeware se propaga a

otros dispositivos conectados a la acera de Amazon.

3. Un hacker ingresa a una red conectada a Amazon Sidewalk y la utiliza para acceder a información sobre dispositivos conectados.

Audio Wow+

Dispositivo IoT que es un mini micrófono inalámbrico con efectos de sonido.

Funciones:

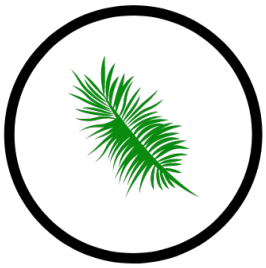
- Teléfono móvil conectado directamente
- Micrófono incorporado
- Monitoreo en tiempo real
- 4 niveles de reducción de ruido
- Cancelar y reemplazar las voces originales
- Graba llamadas telefónicas y transcribe el contenido de la persona que llama y del receptor por separado para facilitar la edición.

Riesgos:

1. Se puede utilizar para grabaciones subrepticias ya que su pequeño tamaño hace que sea fácil de ocultar.
2. Graba ambos extremos de la conversación. La mayoría de los dispositivos solo graban la mitad de la conversación donde el micrófono está presente.

3. Las grabaciones de voz pueden modificarse para crear grabaciones o evidencia de conversaciones que no tuvieron lugar.

¿Qué se puede hacer para detener las amenazas de ciberespionaje /IoT?



Es esencial proteger su información valiosa de las amenazas de IoT. Entonces, ¿cómo puede evitar que su seguridad se vea comprometida?

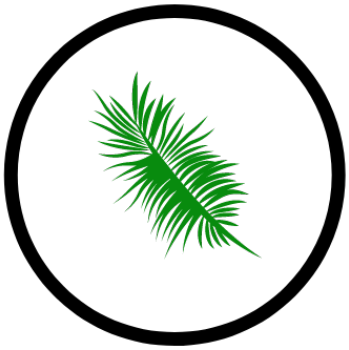
Realice escaneos periódicos de TSCM / CYBER TSCM diseñados para detectar dispositivos móviles maliciosos, teléfonos celulares ocultos y otros dispositivos inalámbricos de escucha y piratería y confirme que nadie ha comprometido sus propios dispositivos personales.

Si desea asegurarse de que su privacidad esté segura, ¡no dude en contactarnos hoy!

A: info@ovationamericas.com o a través de nuestro sitio web en:

www.ovationamericas.com

La seguridad y la privacidad son una cuestión de buenos hábitos personales. Sigamos aprendiendo y manteniéndonos al día sobre temas de ciberseguridad para darnos la mejor oportunidad de evitar costosos hackeos y estafas.



OVATION
AMERICAS