¡Cuidado con los regalos envenenados! Las contraseñas débiles convierten los dispositivos IoT en vulnerables a los ataques

2 enero de 2018

- **En 2015, Kaspersky Lab analizó aleatoriamente 8 dispositivos IoT y la mitad no eran seguros. La seguridad no ha mejorado ya que dos años después, el resultado sigue siendo idéntico**

- **La mitad de los dispositivos pueden verse comprometidos debido a la falta de vigilancia del proveedor en la configuración de contraseñas**

Los dispositivos inteligentes conectados se consideran instrumentos que pueden hacer nuestras vidas más fáciles. Pero ¿hasta qué punto son realmente seguros? En 2015, los analistas de Kaspersky Lab examinaron las amenazas que se pueden encontrar detrás del internet de las cosas (IoT). Los resultados fueron tan preocupantes que, dos años después, se ha vuelto a realizar el mismo análisis. De 8 dispositivos IoT seleccionados al azar, desde una plancha inteligente a un vehículo espía inteligente, la mitad fueron hackeados gracias a la debilidad de las contraseñas (cargador inteligente, asistente personal doméstico, cafetera y cámara IP).

Los dispositivos IOT tienen conectividad de red y están equipados con tecnología integrada que les permite interactuar entre sí o con el entorno. Debido a la gran cantidad y variedad de dispositivos disponibles, el IoT se ha convertido en un objetivo muy atractivo para los cibercriminales. Esto incluye, entre otros, el récord de ataques DDoS lanzados en 2016 con la ayuda de una red botnet masiva, formada por enrutadores, cámaras IP, impresoras y otros tipos de dispositivos. Al hackear con éxito dispositivos IoT, los ciberdelincuentes pueden chantajear a las personas o espiarlas. Otros vectores puedes todavía ser más peligrosos. Por ejemplo, los dispositivos domésticos pueden utilizarse para realizar actividades ilegales, o un cibercriminal que haya obtenido acceso a un dispositivo IoT podría llegar a chantajear y espiar a su propietario o extorsionarlo. El dispositivo infectado puede incluso llegar a romperse, aunque claramente no es lo peor que puede llegar a suceder.

Teniendo todo esto en mente, los analistas de Kaspersky Lab decidieron comprobar si los estudios sobre productos inteligentes IoT y sobre los incidentes que se han ido produciendo, han cambiado el panorama de la seguridad. Para encontrar la respuesta, analizaron de nuevo varios dispositivos inteligentes seleccionados al azar, entre los que se encontraban un cargador inteligente, un coche de juguete controlado desde una aplicación, un asistente personal (Smart home hub) – nodos que unen en un mismo lugar el intercambio de datos entre múltiples dispositivos inteligentes independientes –, una cafetera inteligente, un aspirador inteligente, una plancha inteligente, una cámara inteligente y un reloj inteligente.

Los resultados han sido realmente preocupantes: de los 8 dispositivos examinados sólo 1 llegó a satisfacer las exigencias de seguridad de los analistas.

Además, la mitad de los dispositivos podrían verse comprometidos debido a la falta de vigilancia del proveedor en la configuración de contraseñas. Esto incluía tener una contraseña predeterminada y la imposibilidad de cambiarla, mientras que en algunos casos la contraseña incluso había sido unificada para todos los dispositivos durante su fabricación.

"En Kaspersky Lab hemos estado monitorizando durante años la ciberseguridad de los dispositivos inteligentes y hemos notado unos crecientes niveles de vigilancia de los fabricantes que han ayudado a disminuir el volumen de dispositivos inteligentes inseguros. Sin embargo, el problema sigue ahí y los dispositivos inteligentes aún pueden perjudicar a sus propietarios, lo que nos sugiere que todavía hay mucho trabajo por hacer conjuntamente por parte las empresas de ciberseguridad y los fabricantes de dispositivos conectados", comenta Oleg Zaitsev, experto en seguridad de Kaspersky Lab.

Los analistas de Kaspersky Lab aconsejan a los usuarios tomar las siguientes medidas para protegerse ante la compra de dispositivos inteligentes vulnerables:

1. Antes de comprar un dispositivo IoT, busca en Internet noticias existentes sobre cualquier vulnerabilidad. El Internet de las cosas es un tema muy candente, y muchos analistas están haciendo un excelente trabajo identificando problemas de seguridad en productos de este tipo: desde cámaras para bebés hasta rifles controlados mediante aplicaciones. Es probable que el dispositivo que vayas a comprar ya haya sido examinado por analistas de seguridad y, a menudo, es posible averiguar si los problemas detectados en el dispositivo han sido parcheados o no.

2. No es siempre una buena idea comprar los productos que acaban de salir al mercado. Junto con los fallos estándar que se suelen encontrar normalmente en productos nuevos, es bastante posible que los dispositivos lanzados recientemente contengan problemas de seguridad que aún no han sido descubiertos.

3. Al escoger dónde queremos que nuestra vida sea un poco más inteligente, debemos considerar los riesgos de seguridad existentes. Si nuestra casa es donde almacenamos muchos artículos de valor material, probablemente sería una buena idea instalar un sistema de alarma profesional que pueda reemplazar o complementar el sistema de alarma para el hogar ya controlado por una aplicación, o configurar el sistema existente de forma que cualquier vulnerabilidad potencial no afecte su funcionamiento.

Para superar estas amenazas, Kaspersky Lab ha presentado una versión beta de su solución para el hogar "inteligente" e Internet de las Cosas: el escáner de Kaspersky para el IoT. Esta aplicación gratuita para Android, escanea la red Wi-Fi doméstica e informa al usuario sobre los dispositivos conectados y su nivel de seguridad.

Sobre Kaspersky Lab

Kaspersky Lab es una empresa de ciberseguridad que celebra su 20 aniversario en 2017. El profundo conocimiento de las amenazas y la experiencia en seguridad de Kaspersky Lab se está continuamente transformando en soluciones de seguridad y servicios para proteger a empresas, infraestructuras críticas,

gobiernos y consumidores en todo el mundo. El extenso portfolio de seguridad incluye su reputada solución de protección de dispositivos finales junto con un número de soluciones de seguridad y servicios para combatir sofisticadas amenazas digitales en constante evolución. Más de 400 millones de usuarios son protegidos por las tecnologías de Kaspersky Lab y ayudamos a 270.000 clientes corporativos a proteger lo que más les importa. Más información en www.kaspersky.es

Síguenos en:

http://twitter.com/#!/KasperskyES

http://www.youtube.com/user/kasperskyespana

http://www.facebook.com/kasperskyes


http://blog.kaspersky.es/

Para más información, contactar con:

eVerythink PR
Virginia Frutos
Tel. +34 91 551 98 91
Mov: 670 502 902
Email: virginia.frutos@everythinkpr.com

Kaspersky Lab Iberia
Vanessa González
Directora de Comunicación
Tel. +34 91 398 37 52
Email: vanessa.gonzalez@kaspersky.es