Publicado en Ciudad de México el 04/09/2018

# [Avast: al menos 32.000 negocios y hogares inteligentes en riesgo de filtrar datos](http://www.notasdeprensa.es)

## Avast describe cinco maneras en las que los ciberdelincuentes pueden aprovecharse de los servidores MQTT para hackear hogares

 Una nueva investigación de Avast (LSE: AVST), el líder global en productos de seguridad digital, encontró que existen más de 49.000 servidores Message Queuing Telemetry Transport (MQTT) visibles públicamente en internet debido a la mala configuración del protocolo MQTT. Esto incluye más de 32.000 servidores sin contraseña, lo que los pone en riesgo de filtrar datos. El protocolo MQTT se usa para conectar y controlar dispositivos domésticos inteligentes por medio de hubs de hogares inteligentes. Al implementar el protocolo MQTT, los usuarios configuran un servidor. En el caso de los consumidores, por lo general, el servidor se encuentra en una PC o minicomputadora, como Raspberry Pi, a la que los dispositivos pueden conectarse y con la que pueden comunicarse. Si bien el protocolo MQTT es seguro, pueden surgir graves problemas de seguridad si no se implementa y configura bien. Los ciberdelincuentes pueden tener acceso total al hogar y descubrir si los propietarios se encuentran allí; manipular los sistemas de entretenimiento, asistentes de voz y dispositivos domésticos, así como también ver si las puertas y ventanas inteligentes están abiertas o cerradas. Bajo ciertas condiciones, los ciberdelincuentes incluso pueden rastrear la ubicación del usuario, lo que amenaza muy seriamente tanto su privacidad como su seguridad. “Es aterradoramente sencillo acceder y controlar un hogar inteligente porque aún hay muchos protocolos inseguros que se remontan a una era tecnológica pasada en la que la seguridad no era una prioridad”, afirmó Martin Hron, investigador en seguridad de Avast. “Los consumidores deben tomar conciencia de que estos problemas pueden surgir cuando conectan dispositivos que controlan sectores de su casa con servicios que no llegan a comprender completamente, y de la importancia de configurar adecuadamente sus dispositivos”. Martin Hron describe cinco maneras en las que los hackers pueden aprovecharse de servidores MQTT mal configurados: Los servidores MQTT abiertos y desprotegidos pueden encontrarse mediante el motor de búsqueda ShodanIoT y, una vez conectados, los hackers pueden leer mensajes transmitidos utilizando el protocolo MQTT. La investigación de Avast muestra que los hackers pueden, por ejemplo, leer el estado de los sensores de una puerta o una ventana inteligente y ver si las luces están prendidas o apagadas. En este caso en particular, Avast también encontró que personas extrañas podrían controlar dispositivos conectados o, al menos, contaminar los datos usando el protocolo MQTT. Así, por ejemplo, un atacante podría enviar mensajes a la central para abrir la puerta del garaje. Incluso si un servidor MQTT está protegido, Avast encontró que era posible hackear un hogar inteligente dado que, en ciertos casos, el tablero usado para manejar el panel de control del hogar se ejecuta en la misma dirección IP que el servidor MQTT. Muchos usuarios utilizan la configuración predeterminada del software de la central que controla su hogar inteligente y éstas no suelen estar protegidas con una contraseña, lo que significa que un hacker puede obtener acceso total al tablero y así controlar cualquier dispositivo conectado. Aun si el servidor MQTT y el tablero están protegidos, Avast descubrió que en el caso del software de una central inteligente, Home Assistant, los recursos compartidos por Server Message Block (SMB), abiertos e inseguros, son públicos y, por lo tanto, accesibles para los hackers. SMB es un protocolo para compartir archivos en redes internas, principalmente en la plataforma Windows. Avast encontró directorios compartidos públicamente con todos los archivos de Home Assistant, incluidos los de configuración. Entre los archivos expuestos había uno que contenía contraseñas y claves guardadas en texto sin formato. Las contraseñas almacenadas en el archivo de configuración pueden permitirle a los ciberdelincuentes controlar totalmente un hogar. Los propietarios pueden utilizar herramientas y aplicaciones para crear un tablero para un hogar inteligente basado en MQTT y así controlar los dispositivos conectados. Una aplicación en especial, MQTT Dash, permite a los usuarios crear su propio tablero y panel de control para gestionar los dispositivos inteligentes que utilizan MQTT. Los usuarios tienen la opción de publicar en este servidor la configuración que definieron en el tablero y así reproducirla sin problemas en todos los dispositivos que deseen. Si el servidor MQTT usado es inseguro, cualquiera puede acceder fácilmente al tablero del usuario y hackear el domicilio. Avast también descubrió que el MQTT puede, en ciertas instancias, permitir que un hacker rastree la ubicación del usuario, dado que estos servidores habitualmente se concentran en datos en tiempo real. Muchos de ellos están conectados a la aplicación móvil llamada OwnTracks. Esta aplicación está diseñada para que los usuarios compartan con otros su ubicación, pero también sirve para que los propietarios de hogares inteligentes permitan que sus dispositivos inteligentes sepan que se están acercando al domicilio y, entonces, se activen (por ejemplo, el caso de lámparas inteligentes que se encienden en ese momento). Para configurar la función de rastreo, los usuarios tienen que configurar la aplicación conectándola a un servidor MQTT y exponer ese servidor a internet. Durante este proceso, no se requiere que los usuarios definan credenciales para iniciar sesión, lo que implica que cualquiera puede conectarse al servidor MQTT. Los hackers incluso pueden leer mensajes que incluyan el nivel de batería del dispositivo, la ubicación del usuario determinada por la latitud, la longitud y la altura y la marca de hora para esa ubicación. La investigación completa de Avast se puede encontrar en el blog. Acerca de AvastAvast (LSE: AVST) es el líder global en productos de seguridad digital. Con más de 400 millones de usuarios en línea, Avast ofrece productos con las marcas Avast y AVG que los protegen de amenazas en internet y el panorama de amenazas de Internet de las Cosas que está en constante evolución. La red de detección de amenazas de la empresa está entre las más avanzadas del mundo, y utiliza tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital Avast para dispositivos móviles, PC o Mac están clasificados como los mejores y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de CVC Capital Partners y Summit Partners, que son sociedades de inversión de capital privado líderes en el mundo. Visitar: www.avast.com.

**Datos de contacto:**

Marketing Q

Agencia de Relaciones Públicas

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-al-menos-32-000-negocios-y-hogares](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: E-Commerce Ciberseguridad Recursos humanos Dispositivos móviles Ciudad de México



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