Publicado en Madrid el 19/07/2018

Las contraseñas WiFi WPA2 siguen siendo completamente seguras pese a los ataques Krack, según Siliceo

Como consecuencia de que recientemente han salido en prensa numerosos avances de información relativa a los nuevos fallos de seguridad detectados con los ataques KRACK contra seguridad WiFi WPA, se ha desencadenado un inusual interés por la seguridad de las transmisiones WiFi y las contraseñas WiFI. Cuidar la seguridad y conocer como funcionan los equipos de comunicación que se usan a diario está muy bien pero no hay que tener miedo, las redes WiFi son tan seguras como siempre

Desde diversos medios se ha informado de que la corporación Wi-Fi Alliance está trabajando para impulsar el nuevo sistema de seguridad WPA3 al mismo tiempo que asegura que el protocolo WPA2 actual es seguro y se puede mejorar continuamente con actualizaciones del software o firmware, por lo tanto, en espera de nuevos avances la seguridad WPA2 es completamente segura.

La información publicada hasta ahora ha sido en su mayoría un poco alarmista, sin embargo los expertos aseguran que los router y sistemas de seguridad WiFi WPA2 siguen siendo completamente seguros, o por lo menos los más seguros que existen en la actualidad, porque sacar las claves WiFi de un router WPA2 sigue siendo imposible, sin un descuido del usuario.

Las contraseñas WiFi WPA no corren ningún peligro. En las características definidas en los ataques KRACK hay cuatro claves que según los expertos en seguridad hacen que este ataque no pueda usarse nunca para vulnerar la seguridad de los datos transmitidos por WIFi en la mayoría de los hogares españoles, que son estos:

Con KRACK nunca se puede robar la clave WiFi. Con este famoso ataque nunca se consiguen la contraseña o clave WiFi del router. Este ataque no descifra la contraseña, pero si puede espiar o hacer copia de los datos, email, fotos o páginas web visitadas a través de la conexión WiFi.

La vulnerabilidad KRACK recientemente detectada se ha usado solamente a nivel de investigación, el código y los recursos necesarios para llevarla a cabo no está disponible a nivel de usuario. Ninguno de los vecinos puede hacer un ataque KRACK con un PC convencional, solo se puede realizar con una supercomputadora que cuesta miles de euros, mucho trabajo y mucha dedicación.

El ataque KRACK no funciona contra dispositivos Windows o Apple, todos los usuarios de estos sistemas operativos pueden estar completamente seguros.

Android puede tener un problema de seguridad WiFi, pero si el router que provee a los equipos de Android es seguro, el ataque KRACK también es imposible. Además desde marzo de 2018 ya se están

fabricando dispositivos Android que incorporan la nueva generación de WiFi 802.11ax con cifrado WPA3, que previene los ataques KRACK.

¿Qué es un ataque Krack contra WPA2?
El descubrimiento reciente de esta nueva vulnerabilidad, o método para hackear wifi, ha sido un mérito de los estudios del experto en seguridad Mathy Vanhoef. Este autor publico un avance de sus descubrimientos en octubre de 2017 avisando de cómo la seguridad del protocolo WPA2 se puede vulnerar con los ataques conocidos como KRACKs (Key Reinstallation Attacks).

En este tipo de ataques para robar datos WiFi el atacante consigue engañar a la víctima manipulando los mensajes de “handshake” que envía un dispositivo cuando se conecta por WiFi con cifrado WPA2. Así el hacker consigue acceder y guardar una copia de esos paquetes y así tener acceso a un archivo que contiene la password WiFi para más tarde intentar descifrar claves wifi contenidas en ese archivo.

Pero es importante saber que con KRACK no pueden robar la WiFi, pero si se pueden usar para espiar conversaciones y teóricamente para enviar virus o malware a través de la red para infectar equipos o servidores.

Medidas de seguridad a nivel de usuario contra ataques KRACK
En principio no es necesario hacer nada, ni siquiera cambiar contraseña WiFi al router. Los router y equipos Windows están seguros contra estos ataques, pero como siempre es conveniente estar atentos a las actualizaciones que recomienda el fabricante. Lo único importante es verificar la configuración del router para asegurarse que se usa el protocolo WPA2 y no el WPA-TKIP.

Pero como las consultas sobre seguridad WiFi han aumentado, para intentar resolverlas en el blog de novedades en productos WiFi de Silíceo Online se dan recomendaciones de cómo cambiar contraseñas WiFi y poner una completamente segura.

Como es ya muy conocido no existe una contraseña que sea indescifrable, pero sí contraseñas que duran mucho tiempo contra todo tipo de ataques si son largas y complicadas. Una contraseña WiFi de 9 caracteres ya es muy difícil de descifrar, pero, una contraseña de 11 caracteres que combine letras, números y símbolos, tardaría años y una de 12 caracteres, muchos, muchos años de ataque continuado de un hacker para descifrarla.

La explicación de porqué una contraseña larga es indescifrable es que los cálculos que hacen ordenadores rápidos y potentes contra una contraseña corta, se puede averiguar en minutos, pero una larga necesita más tiempo para ser descifrada, y una compleja de 12 caracteres con símbolos, números y mayúsculas, necesitará tanto tiempo, que puede durar toda la vida, descifrar claves wifi era fácil hace muchos años con la seguridad WPE, pero hoy en día no, ya no se ve ningún dispositivo que use seguridad WPE.

Desde Silíceo Tienda Online, la web especializada en venta de router y antenas WiFi comunican que la

vulnerabilidad KRACK ha impulsado el interés por la seguridad WiFi más de lo que nunca antes había preocupado a los consumidores. Pero hay que destacar que tanto los dispositivos Linux como Android, que eran vulnerables ante los ataques KRACK, están publicando parches y actualizaciones consiguiendo solucionarlo en el primer semestre de 2018. Además, para los usuarios de MAC OS, iPhone o Windows el riesgo real nunca ha existido.

Además el ataque no afecta nunca a los router, sino a los móviles y tablets, por lo que el ataque solo puede hacerse con un equipo WiFi cercano a la ubicación del móvil. El ataque KRACK que sea dirigido contra un smartphone, sería, en teoría, tan costoso y necesitaría tanto tiempo continuado de trabajo, que hace imposible que cualquiera pueda ejecutarlo. Lo que sí es evidente es que los espias, o agentes secretos con equipos altamente sofisticados podrían usarlo. Por lo tanto la tan famosa vulnerabilidad KRACK está solo a disposición de investigadores “nivel experto” como los de las películas de espías, es decir, nada nuevo sobre la tierra.

La mayoría de las empresas de tecnología como Microsoft o Google se han limitado a recordar a los usuarios que, como siempre, naveguen a través de web seguras con protocolo SSL y HTTPS, sobre todo para comprar o transmitir datos personales como los email. Las web seguras con protocolo SSL, por sus características son webs que están cifradas y por tanto no son accesibles a los hacker. Este tipo de web seguras son reconocidas en los navegadores como Firefox o Chrome con el famoso candado verde y el símbolo de SSL y HTTPS.

Las tiendas de productos WiFi sí que han recomendado actualizar los router de los hogares, pero no por problemas de seguridad, sino para mejorar la eficiencia y la velocidad de transmisión con router que adapten a la nueva tecnología avanzada de WiFi AC. Todos los router de los hogares deberían ser ya de doble banda y velocidad de hasta 1200 Mbps para disfrutar de la máxima velocidad de navegación. Un buen ejemplo de router WiFi para el 2018 es el Tenda AC6 que trabaja con la banda de 5G gracias al Chip de Broadcom. Los chip Broadcom de los router Tenda son los mismos que usa Apple en sus dispositivos WiFi y hasta ahora son los más rápidos y seguros del mercado.

Lo mejor de los router WiFi Tenda, es que se configuran fácilmente, de forma automática con botón WPS o desde una aplicación del móvil. Los desarrolladores de Tenda han hecho que el trabajo de como cambiar la clave del WiFi sea fácil, rápido e intuitivo. Poder configurar un router en 30 segundos, eso si que es un gran avance en seguridad para el hogar, recuerdan desde el blog de Silíceo.

Contacto de prensa
Silíceo Tienda Online
Dirección: C/ Juan Ramón Jiménez 11 09200
Miranda de Ebro – Burgos, España
Tfno: +34 644325286 / +34 947059079
Website: www.siliceo.es

Datos de contacto:
Guillermo

Nota de prensa publicada en: Madrid

Categorías: Nacional Telecomunicaciones Ciberseguridad