ENERG

ENERGÍA SANADORA una transformación sana LA MER

Suscríbete a la revista por sólo $749*
*Precio renovación automática

Tecnología vestible atrae a hackers

Los datos que recogen los dispositivos pueden usarse en extorsiones o robo de contraseñas: Symantec; la conexión bluetooth y las aplicaciones son los puntos más vulnerables de un dispositivo vestible.

Por: Gabriela Chávez | Jueves, 14 de agosto de 2014 a las 06:00

Like 26 Tweet 54 +1 5 LinkedIn 11 Share 91 Email

Texto

Algunos legisladores han propuesto prohibir los dispositivos por cuestiones de privacidad. (Foto: EFE)

CIUDAD DE MÉXICO (CNNExpansión) — Ya sean pulseras, relojes o lentes inteligentes, la tecnología vestible parece ser la nueva tendencia tecnológica que conquistará el gusto de los usuarios, pero esta debilidad por un *gadget* nuevo es una ventana a los ciberataques, advirtió la firma de seguridad Symantec.

Los datos que guarda un *smartwatch* diseñado para medir actividad física son aparentemente inofensivos. ¿Cuántas horas duermes? ¿Cuántos pasos caminaste hoy? ¿Cuántas calorías quemaste? Pero para que estos datos sean útiles deben migrar a un *smartphone* o a la nube a través de una conexión bluetooth o WiFi, y es ahí cuando se abre la oportunidad para un hackeo, explicó el analista de seguridad responsiva para Symantec, Candid Wüest.

"La debilidad más grande de estos dispositivos está en las aplicaciones. El punto central del ataque será obtener la información, los datos y poder rastrear a las personas que los usan. En algunos casos podrían incluso

Existen tres riesgos clave para el hackeo a través del computo vestible, pues más allá de inhabilitar el dispositivo, lo que los cibercriminales quieren es obtener un beneficio económico de los datos robados.

"Si es un alto ejecutivo, lo más rentable para un hacker será obtener los *passwords* de algunas aplicaciones que se usan a través de estos *gadgets*. Muchas de las aplicaciones en el dispositivo están interconectadas con redes sociales como Facebook o Twitter, incluso con tu correo electrónico desde donde pueden acceder a otra información sensible", dijo el experto a CNNExpansión.

Otro riesgo es que se usen algunas de las aplicaciones para sobornar al usuario, haciendo extorsiones a través de sexting usando la cámara del aparato. "Estas aplicaciones pueden ser muy peligrosas porque incluso hay algunas que miden tu actividad sexual. Son datos que no quisieras que fueran públicos".

Además, quien vulnere un dispositivo vestible puede utilizar el geolocalizador o GPS para rastrear al dueño persona.

Riesgo ignorado

Wüest explicó que las aplicaciones que transmiten los datos a un *smartphone* o a la nube son una de las ventanas para hackear un dispositivo vestible, y las conexiones bluetooth 4.0 (de bajo consumo de energía) que utilizan la mayoría de estos equipos podrían ser más privadas, pero los desarrolladores no lo están haciendo.

"Muchos usan bluetooth 4.0 y lo curioso es que éste tiene la opción de hacer privada la conexión de estos dispositivos, para que no se pueda rastrear la IP tan fácil, pero incluso las marcas grandes no tienen esa función (...) tal vez sienten que no lo necesitan porque los usuarios no están exigiendo privacidad", dijo el analista.

Tampoco utilizan mucho sistemas para encriptar datos: 20% de las aplicaciones mandan las contraseñas sin encriptar a la nube, según datos de Symantec, mientras que la firma de ciberseguridad ESET estima que 60% de los fabricantes de computo vestible no encriptan.

Hewlett Packard también *levantó la ceja* ante las vulnerabilidades de este tipo de dispositivos. En un estudio reciente informó que cada *gadget* de este tipo tiene en promedio 25 flaquezas a través de las que los *hackers* pueden vulnerar contraseñas o datos del usuario.

Los dispositivos más conocidos de este mercado como Fitbit, Up de Jawbone, Nike Fuel, Gear de Samsung y otros son completamente rastreables, pero firmas como Fitbit y Jawbone cuentan con sistemas de encriptado de datos sobre la conexión bluetooth.

Aunque los expertos estiman que será dentro de dos años cuando este tipo de ciberataques exploten masivamente, la firma de seguridad argentina ESET ya contabilizó 250 *malwares* operativos para dispositivos vestibles, por lo que la explosión de los hackeos a gran escala podría darse en menos tiempo.

Se estima que la tendencia del cómputo vestible continuará con un crecimiento acelerado a lo largo de los próximos años; según datos de la analista de mercado Gartner, para 2020 habrá un mercado de 30,000 millones de unidades.

CNNExpansión en Facebook y en Twitter Imprimir Email Descargar Comentarios (0)

Artículos relacionados

Errores que pueden matar a los vestibles

La tecnología vestible aún no ha logrado desarrollar un 'gadget' completamente independiente

Google Glass puede robar tu contraseña

Expertos crearon un 'software' que mapea el movimiento de tus dedos y descifra cualquier clave

Tecnología vestible, rumbo a nueva era

Rastrear y monitorear los pasos y movimientos del ser humano fue solo el comienzo para este sector

Cómputo vestible, ¿ventana al espionaje?

La llegada de ropa y accesorios inteligentes aniquila la privacidad, dice David Whitford

El negocio tras la tecnología 'vestible'

La industria trabaja para que los nuevos productos generen ingresos y ganen relevancia

Xiaomi lanza un vestible de 13 dólares

La banda deportiva de la firma china compite con productos similares de más de 100 dólares

Otros enlaces

ENFOQUE: Los seis peores tipos de 'hackers'

ENFOQUE: Evita ser víctima de los 'hackers'

Recomendamos

Otras recomendaciones»

- Lala saldrá de compras por Latinoamérica
- Petróleo 'salpica' al divorcio más caro
- 5 argumentos para subir salario mínimo
- Las 34 'perlas' para asociarse con Pemex
- 27 reglas para ser un mal emprendedor
- 3 indeseables por aumento al minisalario

Alrededor de la web»

- ¿Error? Un presunto soldado ruso publica dos fotos tomadas en Ucrania (CNN México)
- Última llamada del 'Chapo' a su esposa antes de ser recluido (ADN Político)
- La hija de Romero Deschamps presume que vive a todo lujo (ADN Político)
- Científicos investigan qué animal devoró a un tiburón blanco de 3 metros (CNN México)

recomendado por

Zona de comentarios

Comparte ésta liga: http://exp.mx/n006GUJ

Enviar nuevo comentario
Iniciar sesión

Enviar

Términos y Condiciones

0 comentarios

Lo más visto

Las más vistas | Comentadas | Enviadas

- Virus amenaza producción de 'carnitas'
- El 'Dress Code' de las altas ejecutivas
- El FBI investiga a Herbalife
- Pañales para adultos, un mercado en auge
- 'cocina'

Principales Noticias

- Los CEO que aceptan el reto del agua helada
- Nextel incumple pago de deuda
- Las rondas energéticas para Pemex e IP
- 5 'apps' básicas para regresar a clases
- Ferrari GTO, el auto subastado más caro

Michael Page Oportunidades laborales gerenciales y directivas
Importante empresa internacional. - Lázaro Cárdenas, Michoacán
ABOGADO FISCAL
Importante empresa de la industria siderúrgica. - México, D.F.
DIRECTOR DE OFICINA DE ADMINISTRACIÓN DE PROYEC
Fondo líder inmobiliario. - México, D.F.
Compañía internacional alimenticia. - Guadalajara, Jalisco
SUBDIRECTOR AGRÍCOLA
Compañía internacional alimenticia. - Guadalajara, Jalisco
PLANT DIRECTOR
Leader and fast-growing building materials multinational. - Puebla, Puebla
www.michaelpage.com.mx

CNNEXPANSIÓN recomienda
Tecnología
6 trucos para dominar tu iPhone 2ª parte
Patrocinado por Banco BASE

Hija de Robin Williams cierra sus redes sociales

Video y Multimedia
Los grandes momentos de Robin Williams en la pantalla grande
El actor interpretó más de 100 personajes en el cine. Conoce algunos de ellos.
Muere la actriz Lauren Bacall
Robin Williams fue encontrado ahorcado, dice la policía

Hier Handy auftanken!
Jetzt 10% Prepaid-Refill-Rabatt!

Obtén tu MBA en Columbia y CONTINUA CON TUS COMPROMISOS
LEARN ABOUT EMBA - AMERICAS
Columbia Business School AT THE VERY CENTER OF BUSINESS

© 2010 Cable News Network. Turner Broadcasting System, Inc. All Rights Reserved.
© 2006 DERECHOS RESERVADOS EXPANSIÓN, S.A. DE C.V.