CÁNCER NIÑAS FORZADAS A PENSAR EN SER MADRES (HOJA 30) **MÚSICA** EL DISCO PÓSTUMO DE LEONARD COHEN (HOJA 32)

SÁBADO
16 DE NOVIEMBRE
DE 2019

PAPEL

LA REVISTA DIARIA DE EL MUNDO

EL NUEVO OBJETIVO HACKER: TU SALUD

Los hospitales españoles afrontan un nuevo peligro: el robo de datos y la manipulación de pruebas médicas y de dispositivos que pueden hasta provocar la muerte

POR **JORGE BENÍTEZ**
ILUSTRACIONES
ULISES CULEBRO

EPI-DEMIA DIGITAL

CIBER-CRIMEN: ROBOS, SECUES-TROS Y ASESI-NATOS

POR JORGE BENÍTEZ MADRID
ILUSTRACIONES: ULISES CULEBRO

Acudes a una entrevista de trabajo y la empresa que te quiere contratar sabe que un psiquiatra te ha prescrito ansiolíticos para digerir un difícil divorcio. Tienes programada una operación de rodilla y cuando ingresas en el hospital un grupo de ciberdelincuentes bloquea la tecnología del quirófano. Tu cirugía tendrá que esperar. ¿No es suficiente? Vayamos aún más lejos. Eres diabético y un día la bomba que te suministra insulina es manipulada por un criminal. Mueres de un coma diabético.

Estos casos ya no son territorio de la ficción que muestra la televisión y el cine. Son reales.

Lo confirman expertos en ciberseguridad y hasta el mismísimo servicio de inteligencia español (CNI), que en el último informe *Ciberamenazas y Tendencias* a cargo del Centro Criptológico Nacional (CCN) menciona al sector sanitario como objetivo. En España, a fecha de junio de 2018, el CCN había registrado 486 incidentes de los que 314 tuvieron la consideración de nivel crítico y tres con criticidad muy alta.

La salud de los ciudadanos puede sufrir tres tipos de ataque, según detallan especialistas en ciberseguridad consultados por *Papel*: el espionaje a través del robo de información médica confidencial; el secuestro informático de hospitales con el fin de obtener un rescate, y el *hackeo* de dispositivos médicos vitales para una persona como marcapasos, bombas de insulina o neurotrans-misores conectados a control remoto. En caso de deceso, estaríamos ante un *ciberhomicido*.

Incluso hay constancia de códigos informáticos capaces de *crear* tumores de la nada (o eliminarlos) en pruebas de imagen como un TAC o una resonancia magnética para manipular el diagnóstico.

Alerta. **Hay un tema que no está en la agenda política y preocupa mucho al CNI y a muchos informáticos españoles: el sector sanitario está siendo atacado en todo el mundo y necesita de formación y dinero para defenderse. "Examino dispositivos médicos y tienen más agujeros que el Titanic", denuncia un ciberexperto**

Los ciberataques contra instalaciones críticas como las sanitarias son frecuentes. La clave es minimizar sus daños. Neutralizarlos. Una misión complicada porque en el mundo virtual defenderse es siempre más difícil que atacar.

De esta responsabilidad ya es consciente un personal al margen de ejércitos y servicios secretos. «Somos más vulnerables de lo que preveíamos», dijo Carlos Mur, gerente del Hospital Universitario de Fuenlabrada, en unas jornadas celebradas a principios de año cuando aludió a un estudio piloto sobre ciberseguridad en dos hospitales madrileños realizado por investigadores de la Universidad de Oxford.

El mes pasado, el sistema del Laboratorio Referencia de Cataluña (LRC), una entidad privada médica que presta servicios a centros asistenciales públicos de esta comunidad autónoma sufrió el ataque de un virus llamado *CryptoLocker*. Los informáticos tuvieron que aislar el programa del laboratorio para «evitar que la infección afectara a los sistemas de información de los demás centros», según informó el departamento de Salud catalán. Esa misma fuente aclaró que no se registraron pérdidas de datos. Filtraciones que sí se han producido en otros países.

EL VALOR DE TUS DATOS

Hoy la salud es el nuevo oro del ciberespacio. Según expertos consultados por *Papel*, los datos médicos tienen un valor al alza en el mercado negro y se pagan más caros que los números de una tarjeta de crédito o de la Seguridad Social. Un historial sacado de una base de datos generalista puede valer entre 10 y 80 euros, el hurto de un informe de una persona concreta alcanza los 1.500 euros y, si la víctima es un VIP –es decir, un político o un alto directivo de una empresa–, se han registrado ofertas que superan los 100.000 euros en la *dark web* (contenido de internet que no está indexado en los motores de búsqueda tradicionales y que esconde numerosas actividades ilícitas) .

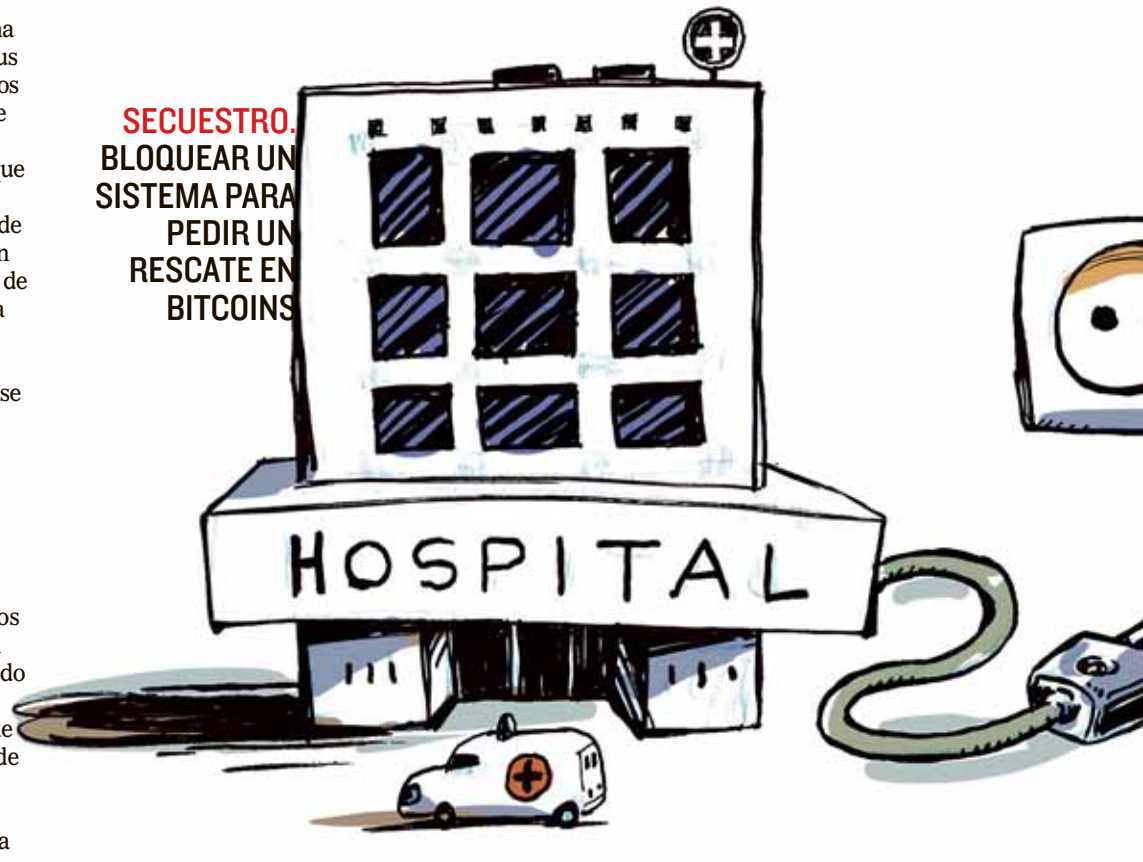
Sin duda uno de los ataques más espectaculares registrados fue el que se produjo en 2018 en Singapur, donde se extrajeron 1,5 millones de datos de pacientes de su sistema sanitario. El propósito de los delincuentes era encontrar información comprometida con la que chantajear al primer ministro Lee Hsien Loong. Más reciente es el ataque sincronizado de este verano a 10 hospitales de Rumanía con el fin de robar expedientes médicos y venderlos en el mercado negro.

Ganar dinero, el chantaje y el espionaje industrial son las razones que hay detrás de estos ciberataques.

En España, fuentes de la Unidad de Investigación Tecnológica de la Policía dicen que no se ha certificado todavía ningún robo sensible de expedientes médicos. En el caso de que este se produjera, no podría mantenerse en secreto, ya que la legislación vigente obliga al hospital afectado a notificarlo al órgano de control en un plazo de 72 horas. Según explica el abogado especialista en comunicación digital Borja Adsuara, si esa violación entrañara un «alto riesgo» debería comunicarse también a los pacientes cuyos datos se hayan visto comprometidos.

En relación a esta obligación, un ciberexperto con experiencia en una multinacional informática se muestra desconfiado: «Hay que tener en cuenta que muchas empresas tienen miedo de denunciar, no quieren dar explicaciones a la Policía o tener una crisis de credibilidad», explica un especialista con experiencia en una importante multinacional informática.

Iván Sánchez es uno de los técnicos que más sabe de protección sanitaria del país. Actualmente es director de la seguridad de la información de la compañía aseguradora Sanitas. ¿Cuál es la muralla



SECUESTRO. BLOQUEAR UN SISTEMA PARA PEDIR UN RESCATE EN BITCOINS

más efectiva para hacer frente a estos ladrones? «La estrategia se debe construir por capas, a través de controles que se complementan y refuerzan cuanto más nos aproximamos al dato. La encriptación mediante clave criptográfica es un mecanismo de seguridad robusto pero debe ir acompañado de controles previos, como alertas ante la fuga de datos sensibles, monitorización, etc. Pero hay que saber que no hay una *bala de plata*, por lo tanto mantener estas capas es fundamental».

Pero la salvaguarda de los datos médicos no sólo implica poner barreras a los delincuentes. El botín sanitario es tan codiciado que también es perseguido –por otros caminos– por colosos tecnológicos como Google, Microsoft y Amazon, que ven en la salud el negocio del futuro.

Según denunció el pasado lunes *The Wall Street Journal*, Google recolectó datos de decenas de millones de estadounidenses dentro de su iniciativa bautizada como P*roject Nightingale* (Proyecto Ruiseñor), un *software* sanitario apoyado en inteligencia artificial, tras haber firmado un acuerdo que se había mantenido en secreto con la compañía médica Ascension. Entre la información adquirida hay historiales en los que se incluyen nombres de pacientes y fechas de nacimiento. La empresa explicó en un comunicado que había «respetado las leyes federales sobre datos médicos». Sin embargo, ni los pacientes ni los médicos habían sido informados de tal uso.

SECUESTRO Y RESCATE

Un simple *post-it* puede desencadenar el armagedón. Es común que los técnicos sanitarios dejen anotadas las contraseñas de los equipos con los que operan a la vista de todos para que las utilicen los del siguiente turno. Igual de peligroso es el empleo de contraseñas genéricas, es decir cuando en lugar de usar su nombre y apellido utiliza alias que emplean muchas personas, «De repente descubres que un paciente ha sido tratado por 'medicoturnonoche' o 'enfermeríaplanta1', esa falta de identidades concretas es confusa en el rastreo de quién es responsable de una determinada acción», cuenta uno de los mayores conocedores del sistema informático en recintos sanitarios del país.

Sin duda el arma más temida por los expertos es «el factor humano», como reconoce Óscar Maqueda, jefe de operaciones de la compañía de ciberseguridad Disruptive Consulting. «Siempre suele estar detrás de un fuga de seguridad. Por eso en España es imprescindible formar al personal de los hospitales y explicar los riesgos informáticos de su trabajo». La mayoría de ataques serios se desatan cuando alguien abre, por ejemplo, un *email* trampa. Se convierte en el *paciente cero* de una pandemia informática. Algo tan peligroso como irse de vacaciones a la playa y dejar las llaves en la puerta.

Dentro de las agresiones a instalaciones, el *ramsonware* es la favorita. Funciona con un tipo de virus que se instala en el ordenador, encripta y secuestra los ficheros y pide un rescate en bitcoins, moneda virtual de muy difícil rastreo. Este ataque lo sufrieron 16 hospitales británico que fueron obligados a cancelar 7.000 consultas por culpa del *Wannacry*, un ciberataque global que en 2017 afectó a 230.000 computadoras de 150 países. En este formato de agresiones sólo hay dos soluciones si no se quiere asumir el riesgo de perder toda esa información sensible: activar un mecanismo de emergencia para detener la propagación del virus (*kill switch*) o pagar a los secuestradores.

CIBERHOMICIDIOS

«He testado muchos dispositivos médicos y tienen más agujeros que el *Titanic*», dice un experto en la materia que denuncia que los fabricantes de neurotransmisores, bombas de insulina, marcapasos y sistemas de imágenes no están concienciados del peligro que tienen sus puntos débiles informáticos.

> EL EXPEDIENTE MÉDICO DE UN PARTICULAR VALE 1.500 EUROS EN EL MERCADO NEGRO. SI EL PACIENTE ES UN VIP MÁS DE 100.000

La posibilidad de un ciberhomicidio es tan real que el ex vicepresidente de EEUU, Dick Cheney, confesó en una entrevista televisiva en 2013 que en una intervención médica a la que fue sometido se desactivaron las funciones inalámbricas de su marcapasos para frustrar un posible intento de asesinato.

Esa amenaza ya había sido denunciada antes. El *hacker* Barnaby Jack anunció que iba a hacer público en una conferencia profesional cómo manipular una bomba de insulina utilizando una antena a cien metros de distancia. Su intención era denunciar el peligro que esconden muchos de estos dispositivos con conectividad inalámbrica.

Barnaby no era un cualquiera: en otro encuentro con la comunidad *hacker* había sido capaz de piratear un cajero automático para que te regalara el dinero.

Días antes de explicar la manera en la que se podía manipular el dispositivo médico, el 25 de julio de 2013, Barnaby Jack fue encontrado muerto en la habitación de su hotel en circunstancias sospechosas.

Los riesgos descubiertos por este *hacker* fueron más tarde confirmados por investigaciones muy serias, como la de la compañía de ciberseguridad Whitescope. «Hay algunos de esos dispositivos que ya se han prohibido en Estados Unidos donde este tema se toma en serio. Mucho más que en Europa, ya que aquí se comercializan», dice un experto que pide no ser identificado.

En ese sentido, José Rosell, especialista en ciberseguridad y socio de S2 Grupo, pide la máxima transparencia. «Hacer públicos estos incidentes permitiría que los políticos se dieran cuenta de los riesgos que hay para la sociedad y de la necesidad de actuar cuanto antes».

Una opinión que comparten todos los profesionales consultados para este reportaje.

Quizás a la espera de la constitución de las Cortes habría que preguntar a los próximos diputados y senadores si usan marcapasos o si son diabéticos.

ASESINATOS. YA ES POSIBLE HACKEAR DISPOSTIVOS MÉDICOS VITALES

ROBO. LOS HISTORIALES MÉDICOS SE VENDEN EN LA 'DARK WEB'