Sala de Prensa

Instituto Nacional de Salud, entre víctimas de ciberataque mundial

Secuestraron información con programa malicioso en 74 países. Objetivo: pedir rescates con bitcoins.

Este viernes fue un día fatal para la ciberseguridad mundial. Empresas y gobiernos de por lo menos 74 países reportaron 45.000 casos de ransomware, o secuestro de datos con un programa malicioso (malware) que bloquea el acceso a sistemas o a archivos. Todo con un objetivo: pedir rescate para liberarlos.

Las primeras informaciones indican que en la gran mayoría de los ataques se hizo uso del programa malicioso Wanna Decryptor o WannaCry, un malware ampliamente conocido por los expertos en seguridad informática.

En los casos reportados, los usuarios se hallaban con una pantalla negra y una ventana emergente con fondo rojo, en la que se les informaba que sus sistemas estaban secuestrados hasta que se hiciera el pago de 300 dólares en bitcoins, moneda digital o 'criptomoneda' preferida por los cibercriminales por su anonimato. Al cambio de este jueves, esa suma equivale a un millón de pesos.

"¡Tus archivos importantes fueron encriptados!", y da dos cuentas regresivas: la primera alerta que en unas pocas horas el monto del rescate subirá.

La empresa rusa de seguridad informática Kaspersky fue la que estimó en más de 45.000 los ciberataques perpetrados. El incidente afectó a países como España, Italia, el Reino Unido, Turquía, Ucrania, Vietnam y Rusia.

La compañía Etek International confirmó tres casos en Colombia. El Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic) le dijo a EL TIEMPO que el Instituto Nacional de Salud también fue víctima del malware y, por prevención, decidió desmontar provisionalmente su página web. (Ver nota anexa).

"Este ransomware infecta a las víctimas explotando una vulnerabilidad de Microsoft Windows descrita y corregida en el Boletín de Seguridad de Microsoft MS17-010. El exploit utilizado, Eternal Blue, fue revelado por Shadowbrokers el 14 de abril. Una vez dentro del sistema, los atacantes instalan un rootkit, que les permite descargar el software para cifrar los datos", explicó Kaspersky Labs en un comunicado.

De Madrid a Londres

Uno de los primeros casos conocidos fue el de la empresa española de telecomunicaciones Telefónica.Empleados de la sede central, en Madrid, reportaron en

redes sociales que se les ordenó apagar los computadores para evitar que se propagara la infección.

La vulnerabilidad, que había sido dada a conocer por Microsoft el 14 de abril, permite la ejecución de código remotamente si se envía un mensaje manipulado al servicio.

Representantes de Microsoft en Colombia le dijeron a EL TIEMPO que en marzo pusieron a disposición de sus clientes protecciones adicionales contra malware de esta naturaleza, con actualizaciones de seguridad que previenen su propagación a través de diferentes redes. “Los equipos que estén corriendo nuestro software de antivirus gratuito y tengan habilitado Windows Update están protegidos”, aseguraron.

Otro blanco de los ataques fue el Servicio Nacional de Sanidad (NHS) del Reino Unido. Al menos 40 hospitales y entidades británicos se vieron afectados, lo que obligó a desviar ambulancias y a suspender citas programadas.

Un portavoz del hospital Saint Bartholomew de Londres dijo que estaban sufriendo “problemas informáticos graves” y retrasos en sus cuatro establecimientos. Sin embargo, aclararon que los datos encriptados no comprometen información clínica de los pacientes. Un incidente similar afectó, en febrero, a un hospital de Los Ángeles, que terminó pagando a los delincuentes.

Entre los archivos ejecutables que llevan la infección están diskpart.exe, tasksche.exe, wannacry.exe y @WannaDecryptor@.exe, indicó Etek. La web del proyecto www.NoMoreRansom.org ofrece asistencia a los afectados.

Instituto Nacional de Salud resultó afectado

Al cierre de esta edición, en el país se habían confirmado tres incidentes relacionados con el ataque. Diego Jiménez, consultor de la firma de seguridad Etek International, comentó que “como está pintando el panorama, vamos a ver muchos más casos”.

En la tarde de este viernes, Juanita Rodríguez, directora de Estándares y Arquitectura TI del Ministerio de Tecnologías de la Información (Mintic), declaró a este medio que “una entidad pública” fue vulnerada con este ataque. “El programa malicioso penetró cuatro equipos, los cuales fueron atendidos inmediatamente”, añadió.

EL TIEMPO logró establecer que se trató del Instituto Nacional de Salud, adscrito al ministerio de ese ramo. Fuentes de la organización confirmaron que, luego de hallar rastros de código malicioso en cuatro de sus servidores, acogieron la recomendación de la cartera TIC y suspendieron los servicios de su página web hasta el lunes 15 de mayo, como medida de prevención.

La decisión no tuvo efectos significativos en la mayoría de los servicios, excepto uno: el de trasplantes, ya que la Red Nacional que centraliza la ubicación, asignación y, sobre todo, los turnos de los trasplantes en el país , usa los recursos del instituto.

Mientras retorna la normalidad, el servicio se prestará por vía telefónica, indicó la entidad.

La cartera TIC informó que la entidad en cuestión detectó el código malicioso a media mañana de ayer.

Otra entidad afectada habría sido el Ministerio de Justicia, cuya página web (www.minjusticia.gov.co) estaba off line anoche, según se indicó, por una similar "medida de prevención".

Álex Durán, jefe del Centro Cibernético Policial, aseguró que el malware en Colombia está creciendo de manera exponencial. "Los ataques en el país se han incrementado en el último año en un 114 por ciento. No necesariamente se trata de una persona con conocimiento en sistemas, también se puede considerar como un servicio que se paga. "A los colombianos los están atacando a través de las plataformas de Gobierno. Se han detectado correos falsos con invitaciones de la Dian, boletines ficticios de la Policía o citaciones a juzgados", añadió.

El Centro Cibernético Policial empezó a registrar casos desde el 2015. Ese año hubo 13 afectados. Pero 12 meses después, el número se multiplicó 600 por ciento: 84 casos. Al cierre de febrero del 2017, ya iban 22, con lo que cabe esperar que el año termine con más de 100. Es un número representativo, porque no todos los casos son notificados a la Dijín.

Actúe para proteger a su empresa

Aislar de la red a los equipos con Windows XP y actualizar los que tengan Windows 7 en adelante son algunas de las principales acciones que el Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic) y los expertos recomiendan a las empresas como medidas de prevención.

Fabián Zambrano, director del DigiSoc de la firma Digiware, señala que es necesario instalar siempre los parches oficiales (actualizaciones que cierran vulnerabilidades y corrigen errores).

"Para las organizaciones que tienen la dificultad de aceptar los parches, deben hacer uso de infraestructura de parchado virtual, que no se aplica directamente dentro del sistema, pero le hace ver a un agente externo como si así fuera", explica.

El especialista reitera que las compañías deben hacer backups de sus archivos y contar con elementos de control de seguridad como antivirus de última generación y sistemas de planificación de recursos empresariales (ERP, su sigla en inglés), que permiten la integración de operaciones de las empresas.

Pero el papel que juegan los empleados es fundamental. "El usuario debe tener cultura de seguridad para que pueda dudar de los archivos anexos que le envían en correos".

Quienes ya hayan sido afectados pueden comunicarse con los correos contacto@colcert.gov.co; incidentes-seginf@mintic.gov.co y caivirtual@correo.policia.gov.co.

Diario EL TIEMPO, 13 de Mayo de 2017. Página 4