Economía

Cronología de los hechos

FEBRERO DEL 2017
Wikileaks filtra que la Agencia Nacional de Seguridad de Estados Unidos utiliza el método para espiar a organizaciones europeas. La agencia checa Avast confirma una primera versión del virus, llamada WeCry.

14 DE MARZO DEL 2017
Microsoft envió a sus clientes el parche de seguridad MS17-010 el 14 de marzo de este año. En el comunicado, catalogó la actualización de "crítica" y publicó otras 14 actualizaciones enfocadas a mejorar la seguridad de los usuarios y sus dispositivos.

12 DE MAYO
Casi dos meses más tarde, el virus WannaCry cobra vida y la primera víctima en reconocer la infección es Telefónica. A lo largo del día, el ataque se replica 45.000 veces en 70 países. Muchas empresas desconectan preventivamente sus sistemas.

13 Y 14 DE MAYO
El virus llega a más de 150 países, y el número de afectados supera los 200.000, según la Europol. Surge una herramienta para frenar el virus y también Windows lanza nuevos parches. Aún se desconoce quién hay detrás de los ataques.

La seguridad global, amenazada

El virus supera los 200.000 contagios y eleva el riesgo en la vuelta al trabajo

El Gobierno traslada tranquilidad y asegura que en España solo hay 600 casos

NIKLAS HALLEN / AFP

El sistema de salud británico, uno de los sectores en los que el virus se ha extendido con mayor intensidad

LALO AGUSTINA
Barcelona

El virus Wannacry, que aprovecha una falla en la seguridad de Windows para encriptar archivos e inutilizar los ordenadores, amenaza el inicio de la semana laboral después de un fin de semana en el que los informáticos de las empresas han trabajado a destajo. La Europol aseguró ayer que hay alrededor de 200.000 contagios confirmados en 150 países, en lo que supone un éxito sin precedentes en la historia de la ciberdelincuencia.

El virus está totalmente extendido y todo apunta a que se sigue propagando, tanto en su primera versión como en las mutaciones que ya se están reportando. ¿Qué pasará cuando se enciendan hoy los millones de ordenadores asiáticos que han estado apagados desde el viernes, al inicio de la crisis? ¿O cuando se conecten a la red los miles de ordenadores ya infectados? Nadie lo sabe. De momento, no hay valoraciones de daños. La desinformación –probablemente, cargada de un profundo desconocimiento– campa a sus anchas.

Los expertos consultados insisten en las pocas cosas que se pueden tener por seguras. Por ejemplo, recuerdan que si un equipo no está infectado, el riesgo puede evitarse instalando todas las actualizaciones de Microsoft, el fabricante de los sistemas operativos vulnerables. O que la exposición a los *hackers* es mucho menor si se tienen copias de seguridad. Y poco más. "El gusano va a seguir infectando", comenta Ramon Vicens, vicepresidente de ciberamenazas en Blueliv, que añade: "En el mundo hay millones de ordenadores personales que tienen limitaciones a las actualizaciones automáticas, por lo que sólo es cuestión de tiempo que se acaben infectando".

España, según explicó el Instituto Nacional de Ciberseguridad (Incibe), contaba ayer con unas 600 infecciones, de las que menos de una decena habría afectado a empresas de carácter estratégico. Entre las grandes corporaciones, sólo Telefónica lo ha reconocido públicamente, pero hay unas cuantas más en la misma situación o una similar, con varios cientos de equipos afectados, aunque operando todas ellas con aparente normalidad.

El virus ya es global. Se ha cebado especialmente en Rusia, donde se concentran más de la mitad de los ataques. Ningún gran país está al margen, y las autoridades trabajan para intentar detener a los culpables. Ayer trascendió que la noche del viernes se produjo la primera reunión entre el FBI y la Agencia de Seguridad Nacional de Estados Unidos para coordinar las investigaciones. En Europa, la coordinación corre a cargo de la Europol. España se sitúa en el puesto 18.º en el ranking por países infectados, según datos facilitados por el Incibe en la mañana de ayer.

Durante los tres últimos días, las empresas afectadas han estado trabajando para limpiar sus equipos y tratar de entrar en la semana con normalidad. Pero no todo está resultando tan fácil, aseguraron ayer desde una de las empresas contaminadas, que veían todavía un poco prematuro aventurar en qué momento podrían dejar atrás cualquier preocupación por este asunto.

En cualquier caso, pese a la alarma global, tres días después del inicio de la pandemia informática, predomina la tranquilidad. Las tres cuentas de Blockchain donde los piratas informáticos reciben los pagos por parte de los usuarios extorsionados que han cedido al chantaje apenas registraron movimiento ayer. A última hora de la tarde, constaban 125 operaciones por un total de casi 20,2 bitcoins, alrededor de unos 32.500 euros.

Buena parte de esta pobre evolución radica en que tanto las autoridades como los expertos aconsejan no pagar. No hay garantías de que, al hacerlo, se obtengan los resultados deseados. En cambio, la principal lección de la crisis está en la prevención. En España, las administraciones públicas deben cumplir el esquema nacional de seguridad, basado en la ISO 27001, que obliga a adoptar las medidas básicas de protección, como realizar actualizaciones periódicas de los equipos. Pero el sector privado, más allá de lo relativo a la ley de protección de datos, no se encuentran en la misma situación.●

EL LUNES TODO SE ENCIENDE

Tras el fin de semana, llega la hora de volver al trabajo y comprobar si la pandemia remite

AFECTACIÓN EN ESPAÑA

El Gobierno dice que las empresas estratégicas afectadas no llegan a diez

POCA "RECAUDACIÓN"

Hasta ayer sólo se han producido 125 pagos por el equivalente a unos 32.500 euros