El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de unos 150 países

Redacción
BBC Mundo

13 mayo 2017

El programa malicioso usado en el 'ransomware' exige a contrarreloj un pago por la liberación del sitio.

Un ciberataque "de dimensión nunca antes vista" logró este viernes bloquear el acceso a los sistemas informáticos de instituciones estatales y empresas de varios países.

La policía europea, Europol, indicó que el ciberataque era de una **escala "sin precedentes"** y advirtió que una "compleja investigación internacional" era necesaria para "identificar a los culpables".

El domingo se anunció que el ataque afectó a unas 200.000 víctimas en 150 países.

- **Ciberataque masivo a escala global: 5 preguntas para entender qué es y de donde surgió el virus WannaCry**

La campaña masiva de *ransomware*, un ataque en el que los perpetradores piden dinero a cambio de liberar el acceso a los sistemas, también afectó a instituciones de **Reino Unido, Estados Unidos, China, España, Italia, Vietnam y Taiwán**, entre otros.

El fabricante de vehículos Renault señaló que detuvo la producción en sus fábricas francesas como consecuencia del ataque.

> *Este es un ataque cibernético importante que impacta*

organizaciones de toda Europa a una dimensión nunca antes vista

Kevin Beaumont, experto en seguridad

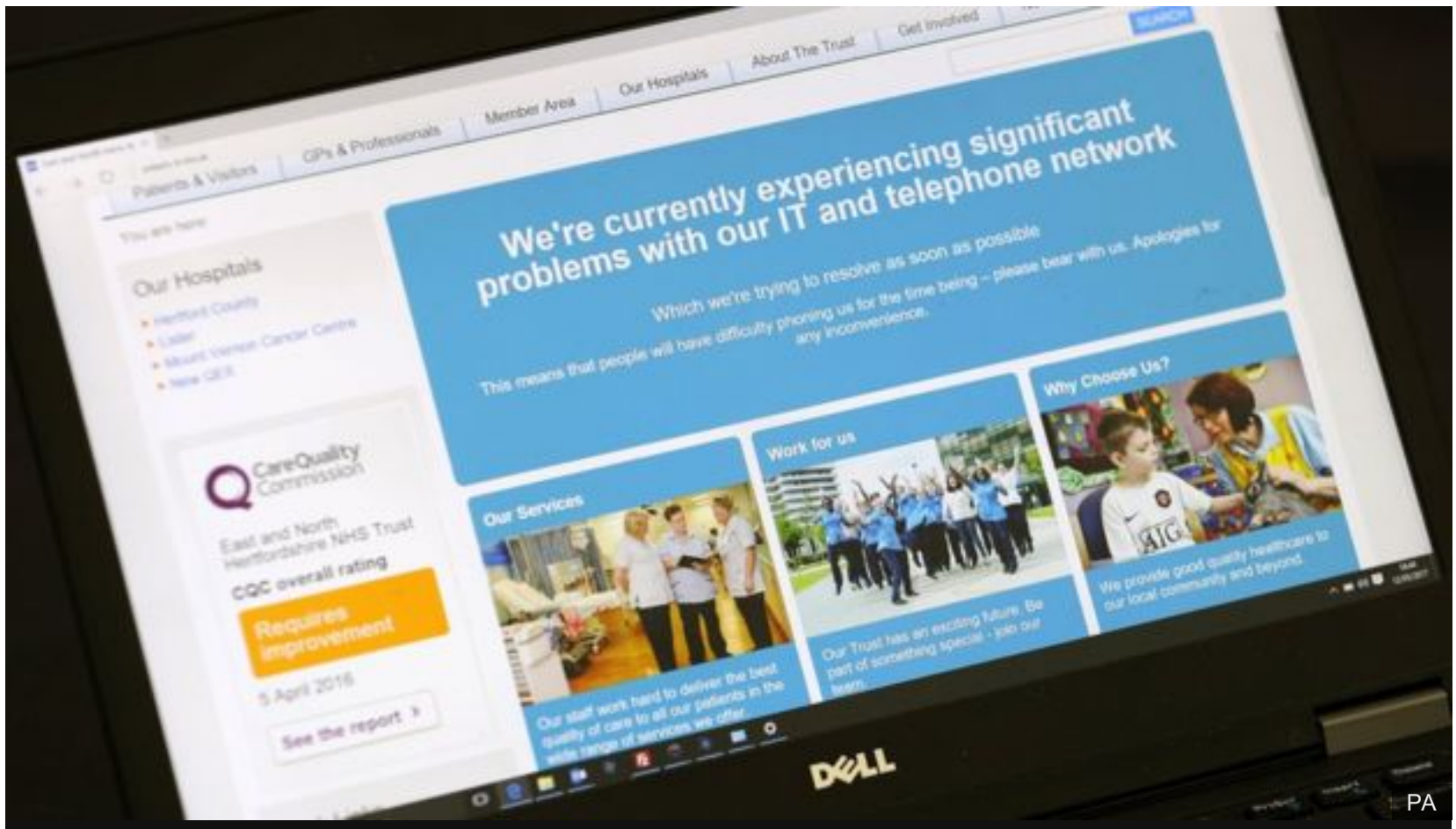
Se informó que las herramientas usadas en el ataque pudieron haber sido desarrolladas por la Agencia de Seguridad Nacional de Estados Unidos (NSA, por sus siglas en inglés).

- **Cómo una fisura en Windows fue el origen del ciberataque de alcance mundial (y por qué muchos culpan a la Agencia Nacional de Seguridad de EE.UU.)**

Hackers se atribuyeron el mes pasado el robo del software, conocido como *Eternal Blue*, y su distribución por internet.

"Este es un ataque cibernético importante, que impacta organizaciones de toda Europa **a una dimensión nunca antes vista**", dijo el experto en seguridad Kevin Beaumont.

"Hemos visto más de 75.000 casos... en 99 países", escribió Jakub Korustek en un blog de la firma de seguridad informática Avast publicado alrededor de las 20:00 GMT de este viernes.



PA

El sitio del NHS británico mostraba problemas para acceder a sus sistema informático y de telefonía.

Horas antes, Costin Raiu, de la tecnológica rusa Kaspersky, había hablado de 45.000 ataques en 74 países.

Raiu describió el virus como **un "gusano" que se estaba autorreplicando y esparciendo a gran velocidad**.

Por su parte, Forcepoint Security señaló que el gusano estaba siendo esparcido por una campaña de correos electrónicos malicioso de hasta 5 millones de *emails*.

- **"Paga o destruimos tus datos": cuáles son los ramsonware "más buscados" por la policía en Europa**

¿Qué piden?

Computadoras en miles de lugares han sido bloqueadas por un programa que demanda el pago de US$300 en la moneda electrónica bitcon para que los sistemas puedan ser liberados.

- **Luego de años en las sombras, el creador de Bitcoin revela su identidad**

Una de las pantallas bloqueadas este viernes mostraba la amenaza de que un pago a cambio de liberar el sistema debía ser completado antes del 15 de mayo o de lo contrario los archivos serían eliminados cuatro días después.

¿QUÉ ES UN RANSOMWARE?

Es un software malintencionado

que restringe el acceso a algunos archivos y

que pide un rescate a cambio

Se transmite como un troyano o un gusano capaz de duplicarse.

Se presenta como un programa inofensivo pero suele infectar el sistema operativo explotando una vulnerabilidad del software y cifrando archivos.

"¡Ups, tus archivos han sido encriptados!", decía el *ransomware*, el cual es conocido como **WannaCryptor** o **WCry**, aunque también es conocido como "WannaCry", en inglés "quieres llorar".

"No pierdas el tiempo, nadie puede recuperar tus archivos sin nuestro servicio de desencriptación", decía el mensaje que supuestamente garantiza la devolución de la información a cambio del pago.

Hasta ahora se desconoce quién puede estar detrás de los ataques y si fueron ejecutados de forma coordinada.

Sin embargo, varios expertos que dan seguimiento a la situación apuntan a las vulnerabilidades dadas a conocer por un grupo conocido como **The Shadow Brokers**, que recientemente afirmó haber robado herramientas de *hackeo* a la NSA.

Un parche para reparar la vulnerabilidad fue liberado por Microsoft en marzo, pero muchos sistemas pueden no haber tenido la actualización instalada, según los expertos.

Las autoridades y los especialistas recomiendan no pagar rescates por ataques informáticos como los 'ransomware'.

Los afectados

Las autoridades en Reino Unido declararon que tenían un "incidente importante" después de que varios hospitales del Servicio nacional de Salud (NHS, por sus siglas en inglés) en Inglaterra y Escocia se vieron afectados.

El personal no pudo acceder a los datos de los pacientes, pero hasta ahora no hay evidencia de que su información personal se haya visto comprometida, según el NHS.

Ello llevó a la cancelación de cotas con pacientes y la suspensión de actividades como intervenciones quirúrgicas.

Entre las empresas españolas afectadas está el gigante de las telecomunicaciones **Telefónica**, que confirmó que estaba lidiando con un "incidente de seguridad cibernética", pero aseguró que sus clientes no se veían afectados.

Las compañías energéticas **Iberdola** y **Gas Natural** también registraron problemas en sus sistemas.

Otra empresa que confirmó que había sido atacada fue la empresa de mensajería estadounidense FedEx, aunque no aclaró en qué lugares hizo efecto el *ransomware*.

"Al igual que muchas otras compañías, FedEx está experimentando interferencia con algunos de nuestros sistemas basados en Windows", dijo la empresa en un comunicado.

En Italia, las computadoras de un laboratorio universitario quedaron bloqueadas por el mismo programa, como mostró un usuario en Twitter.

EPA

La coordinación de algunas ambulancias y los sistemas de registros de consultorios médicos resultaron afectados en Inglaterra y Escocia.

La mayor y más creciente amenaza: Chris Baraniuk, reportero de tecnología de la BBC

El *software* que bloquea la computadora y exige el pago antes de devolverle el acceso al usuario, llamado *ransomware*, es una de las mayores y crecientes amenazas informáticas del mundo.

Ciertamente parece que eso es lo que ha golpeado al NHS en este caso.

Imágenes compartidas en línea, supuestamente de miembros del personal del NHS, muestran un programa que exige el pago de US$300 en bitcoin y que se parece al *ransomware* conocido como WannaCryptor o WCry .

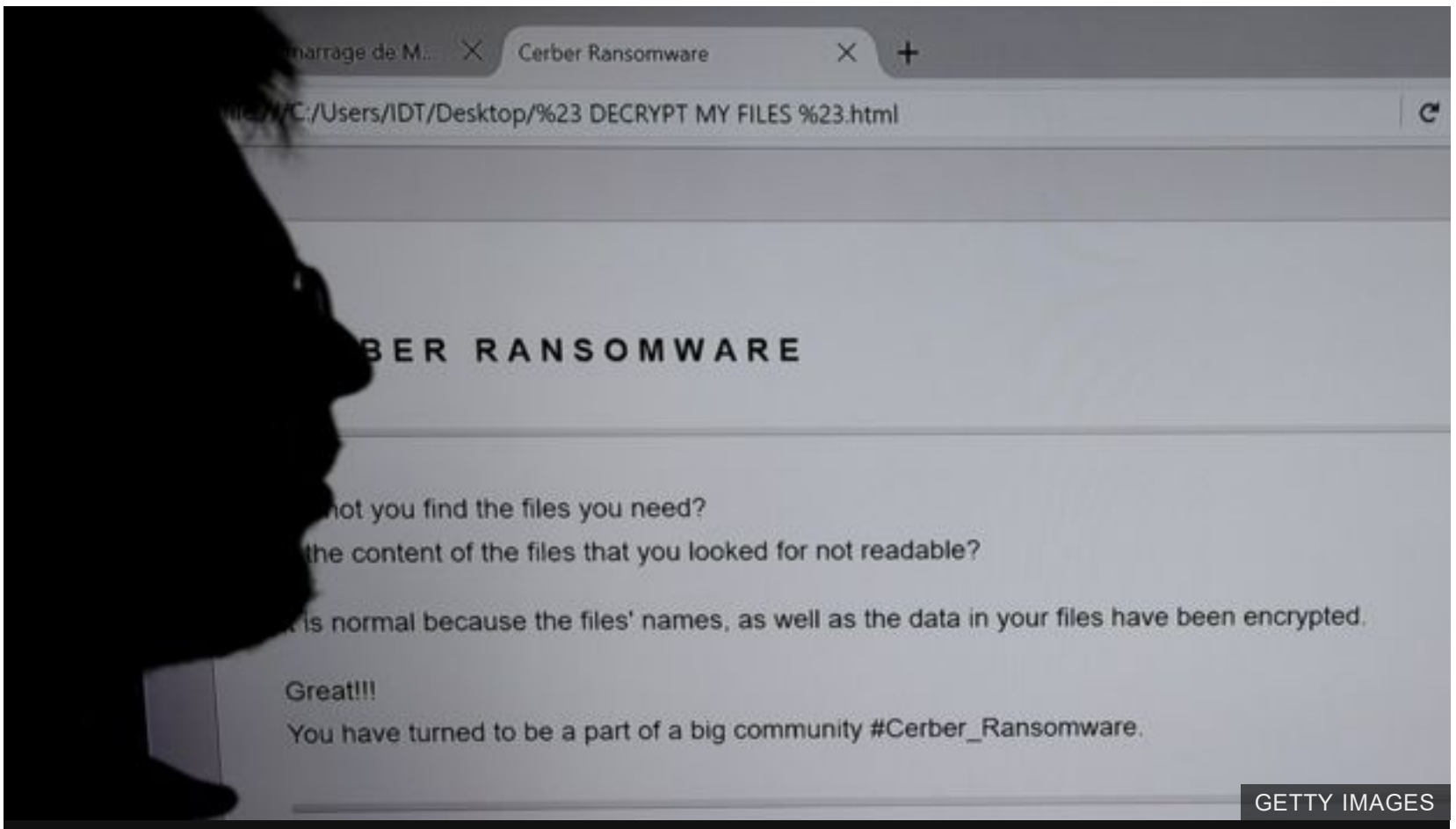
Sin embargo, no hay ninguna indicación de quién está detrás del ataque ni sabemos exactamente cómo infectó los sistemas del NHS.

Los hospitales ya han sido blanco de un software similar antes, como el que golpeó tres hospitales de Estados Unidos el año pasado.

¿Afecta a computadoras personales?

Sí y es una de las trampas que más han crecido entre usuarios de computadoras personales, normalmente a través de correos electrónicos.

Una de las variantes de *ransomware* más extendidas se llama **Locky**.



GETTY IMAGES

La recomendación es no abrir documentos o archivos adjuntos de correos electrónicos de procedencia desconocida.

Se trata de **un virus troyano querecibe la víctima a través de un correo electrónico** que le pide abrir un archivo adjunto con un título similar a "documento de pago" o "recibo".

Una vez abierto, a través del programa Word o en archivo comprimido, los comandos (macros) se ejecutan de forma automática y "toman" el control del ordenador.

Lo siguiente que ve la víctima es una pantalla con instrucciones de pago en bitcoins como los que se vieron este viernes alrededor de mundo.

Otros *ransomware* comunes son **CryptoWall4, PadCrypt o Fakben**.

La recomendación de los expertos para los usuarios comunes es **no abrir archivos adjuntos de procedencia desconocida**.

Temas relacionados

Europa **Ciencia** **Reino Unido** **Tecnología** **Rusia** **Computación** **Estados Unidos** **España**

Compartir Acerca de compartir

Volver Arriba

Contenido relacionado

Cómo una fisura en Windows fue el origen del ciberataque de alcance mundial (y por qué muchos culpan a la Agencia de Seguridad Nacional de EE.UU.)

13 mayo 2017

"Paga o destruimos tus datos": cuáles son los 'ramsonware' "más buscados" por la policía en Europa

28 julio 2016

Principales noticias

"Tienes que ser fuerte, tu hijo está muerto": la conmovedora historia del joven Juan Pablo

Microsoft responsabiliza a la Agencia de Seguridad Nacional de EE.UU. de propiciar el ciberataque

Cómo una fisura en Windows fue el origen del ciberataque de alcance mundial (y por qué muchos culpan a la Agencia de Seguridad Nacional de EE.UU.)

Redacción
BBC Mundo

13 mayo 2017

REUTERS

Kaspersky Lab, una firma de origen ruso, dijo que Rusia fue la más afectada por el ciberataque, seguida por Ucrania, India y Taiwán.

Todo comenzó en abril.

Hace menos de un mes, el grupo de hackers *Shadow Brokers* hizo pública una serie de herramientas de ataque cibernético entre las que se encontraba ***EternalBlue*, un "arma virtual"** que expertos atribuyen a la Agencia de Seguridad Nacional de Estados Unidos (NSA, por sus siglas en inglés).

- **El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de más de 70 países**
- **Ciberataque masivo a escala global: 5 preguntas para entender qué es y de donde surgió el virus WannaCry**

EternalBlue, que es una herramienta que explota una fisura o punto débil en el sistema operativo Windows, de Microsoft, fue "el factor más significativo" del masivo ataque que se vivió este viernes en **al menos 74 países**, según la firma de seguridad cibernética Kaspersky Lab.

El atentado cibernético, cuyos autores todavía no se conocen, logró bloquear el acceso a los sistemas informáticos de instituciones estatales y empresas de alrededor del mundo a través del software maliciosos Ransom:Win32.WannaCrypt.

REUTERS

El cuartel general de la NSA en Fort Meade, Maryland.

Kaspersky Lab, una firma de origen ruso, dijo que Rusia fue la más afectada, seguida por Ucrania, India y Taiwán.

También alcanzó a Estados Unidos y Reino Unido, donde afectó especialmente a su sistema de salud.

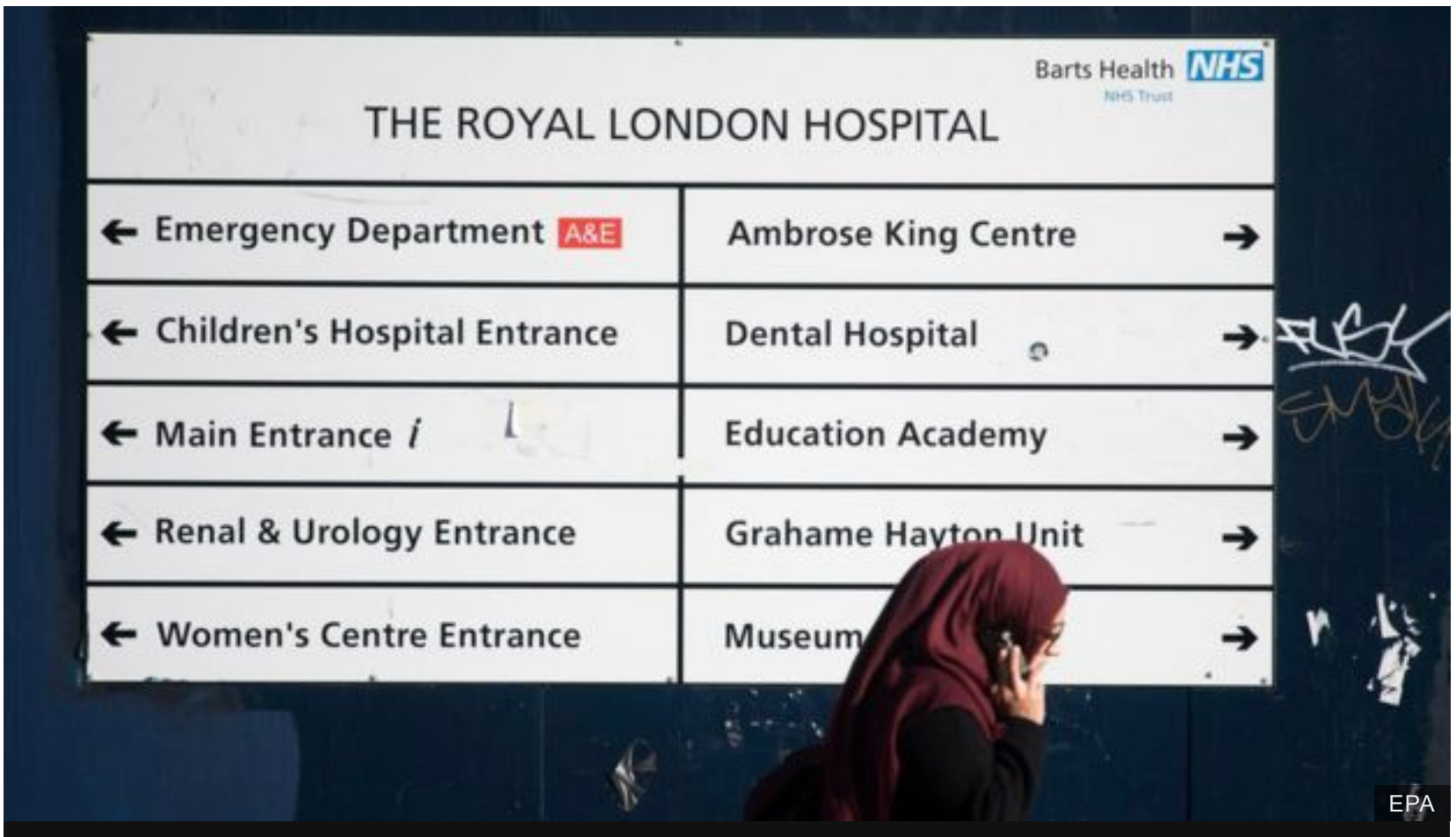
- **Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país**

América Latina y África también sufrieron el ataque, según los últimos reportes de la noche del viernes.

¿Qué hizo la NSA?

Estados Unidos nunca confirmó si el arsenal de ciberataques filtrados por *Shadow Brokers* pertenecían a la NSA o a otras agencias de inteligencia.

Sin embargo, antiguos oficiales de inteligencia señalaron que las herramientas parecían venir de la unidad de "Operaciones de Acceso Personalizado" de la NSA, que se cree se dedica a infiltrarse en las redes de computación extranjeras.



EPA

El ciberataque castigó particularmente al sistema de salud de Reino Unido.

Por ello es que los expertos apuntan a que la ola masiva de ataques del viernes puede ser **la primera vez que una ciberarma desarrollada por la NSA**, financiada por contribuyentes estadounidenses **y robada por un adversario, fue aprovechada por delincuentes informáticos** contra hospitales, empresas, gobiernos y ciudadanos comunes.

"Sería profundamente preocupante si la NSA sabía sobre esta vulnerabilidad, pero no la reveló a Microsoft hasta después de que fue robada", afirmó Patrick Toomey, abogado que trabaja para la Unión Estadounidense por las Libertades Civiles (ACLU, por sus siglas en inglés).

- **¿Cuáles son las armas con las que se combate en el ciberespacio, el nuevo frente de guerra del siglo XXI? (Y qué daño te pueden causar)**

"Estos ataques subrayan el hecho de que las vulnerabilidades serán explotadas no sólo por nuestras agencias de seguridad, sino por **hackers y criminales de todo el mundo**", añadió el experto de la organización civil estadounidense.

Toomey agregó que lo correcto en adelante debe ser alertar y corregir los "agujeros de seguridad", en lugar de explotarlos y almacenarlos.

Por su parte, Edward Snowden, quien también filtró muchos archivos internos de la NSA en junio de 2013, no perdió la oportunidad para cuestionar a la agencia estadounidense.

"A la luz del ataque de hoy, el Congreso debería estar preguntando (a la NSA) si sabe de cualquier otra vulnerabilidad en el software utilizado en nuestros hospitales", escribió el analista en su cuenta de Twitter.

Algunos hospitales de Reino Unido fueron bloqueados al punto que los médicos no podían solicitar los historiales de los pacientes y las salas de emergencia se vieron obligadas a transferir a las personas que buscaban atenciones de urgencia.

Lo sucedido este viernes tiene un antecedente.

Algo similar ocurrió con restos del gusano "Stuxnet", que Estados Unidos e Israel usaron contra el programa nuclear de Irán hace casi siete años.

Partes del código de esa ciberarma aparecen con frecuencia en otros ataques menores desde entonces.

¿Qué dice Windows?

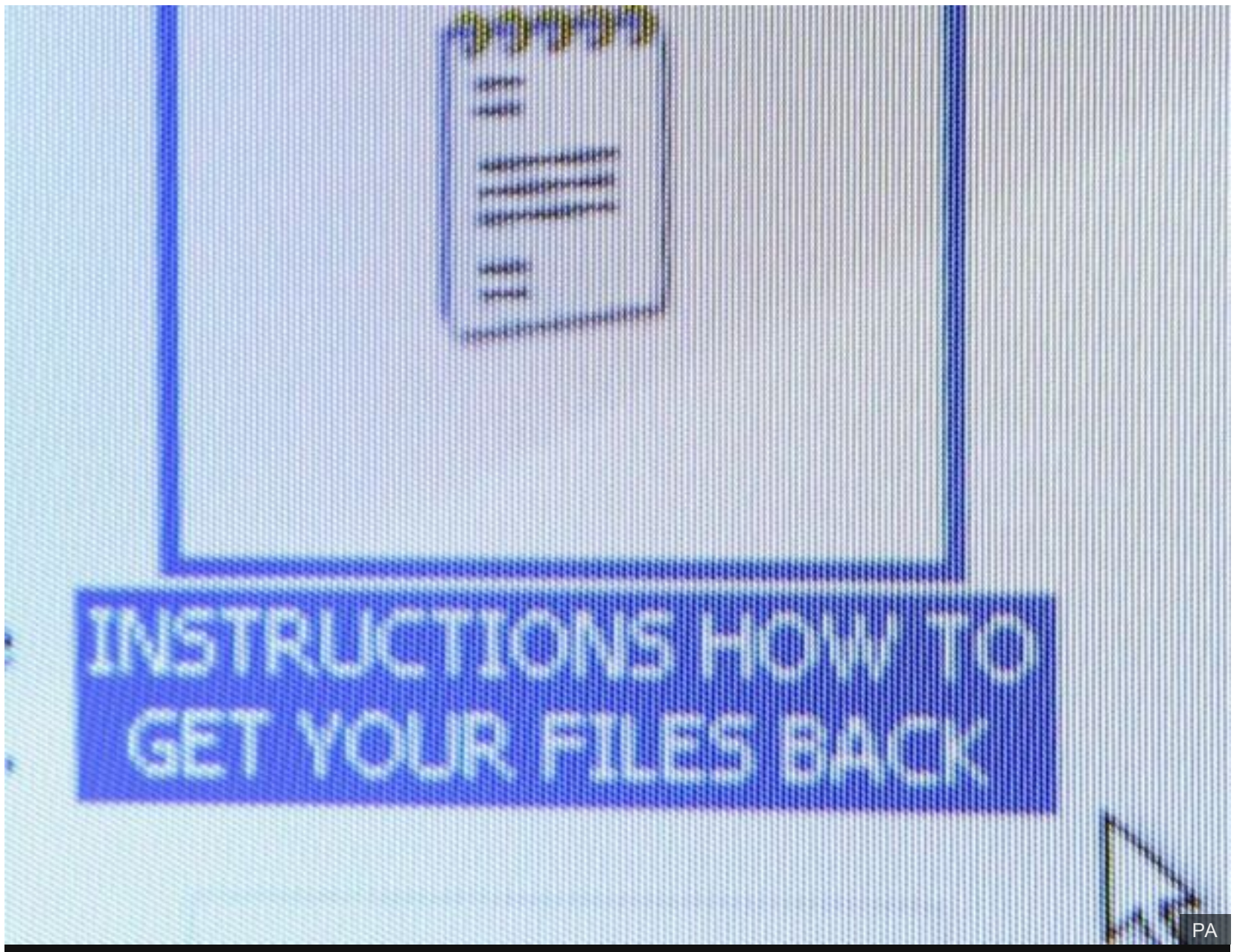
Se conoce que la fisura de Windows fue corregida hace más de un mes, sin embargo **es imposible "parchar" todas las computadoras automáticamente**.

- **¿Se pararía el mundo si internet dejara de funcionar por un día?**

Mucho más en casos como el del Sistema Nacional de Salud de Reino Unido, que sigue operando con Windows XP, un sistema operativo que ya no recibe mantenimiento de Microsoft.

Algunos hospitales de ese país fueron bloqueados al punto que los médicos no podían solicitar los historiales de los pacientes y las salas de emergencia se vieron obligadas a transferir a las

personas que buscaban atenciones de urgencia.



Los ciberdelincuentes reclaman un rescate en bitcoins para devolver los archivos.

Horas después de que el ciberataque se convirtiera en noticia mundial, Microsoft publicó un comunicado breve anunciando nuevas medidas de seguridad.

"El día de hoy, nuestros ingenieros incorporaron **detección y protección contra el nuevo software malicioso** conocido como Ransom:Win32.WannaCrypt. En marzo, pusimos a disposición de nuestros clientes protecciones adicionales contra *malware* de esta naturaleza, con actualizaciones de seguridad que previenen su propagación a través de diferentes redes", señaló el comunicado.

Microsoft señaló que hace todo lo posible para que los nuevos parches lleguen a la mayor cantidad posible de sus clientes.

Pese a los esfuerzos de la gigante de la computación, los entendidos en la materia señalan que lo sucedido **no le hace nada bien a la imagen de Microsoft**.

Pero existe otra consecuencia aún más importante que deja todo esto.

El ciberataque masivo pone en tela de juicio el papel del creciente número de países que están desarrollando y almacenando armas cibernéticas.

Quedó demostrado que en cualquier momento, en un día cualquiera, **ese arsenal puede ser utilizado en contra de sus propios ciudadanos**.

Temas relacionados

Ciencia | Reino Unido | Tecnología | Rusia | Computación | Internet | Estados Unidos

Compartir Acerca de compartir

Volver Arriba

Microsoft responsabiliza a la Agencia de Seguridad Nacional de Estados Unidos de propiciar el ciberataque masivo que afectó al menos a 150 países

Redacción
BBC Mundo

8 horas

El gigante de la informática responsabilizó a la Agencia Nacional de Seguridad estadounidense por lo sucedido.

Un "llamado de atención" para los gobiernos y organizaciones coleccionistas de vulnerabilidades informáticas.

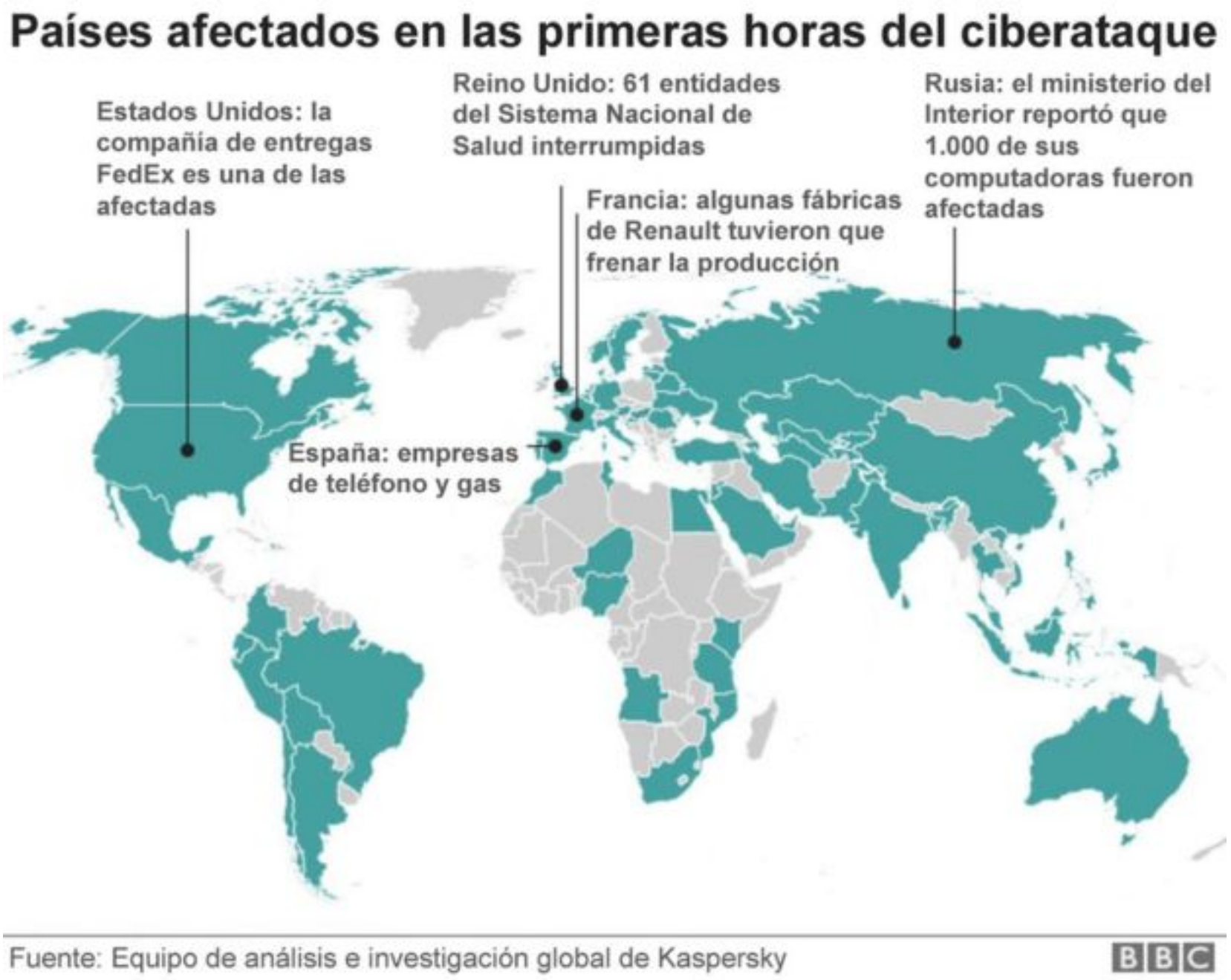
Así calificó Microsoft al ciberataque masivo que comenzó el pasado viernes y ya dejó 200.000 afectados en al menos 150 países.

- **Por qué los expertos creen que otro ciberataque masivo puede ser "inminente" y qué puedes hacer para protegerte**
- **El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de unos 150 países**

El gigante de la informática, además, responsabilizó a la Agencia Nacional de Seguridad estadounidense (NSA, por sus siglas en inglés) por lo sucedido.

"Hemos visto aparecer en WikiLeaks vulnerabilidades almacenadas por la CIA, y **ahora esta vulnerabilidad robada a la NSA ha afectado a clientes en todo el mundo**", señaló el principal asesor legal de Microsoft, Brad Smith.

"El software malicioso WannaCrypt usado en el ataque fue extraído del software robado a la Agencia de Seguridad Nacional en Estados Unidos", señala el ejecutivo.



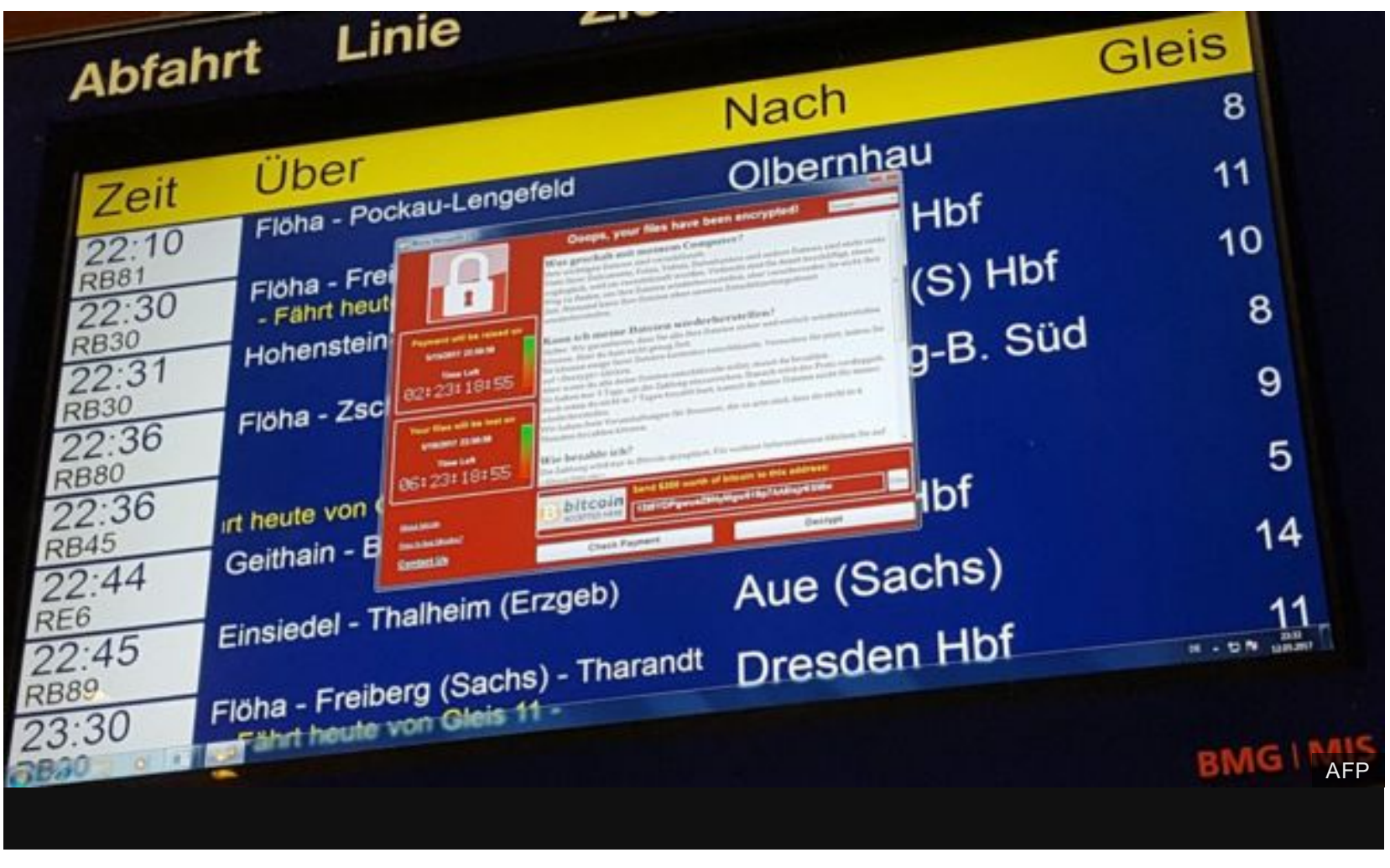
Asimismo, Smith reconoció la "responsabilidad" de Microsoft en la respuesta a esa "llamada de atención" que ha supuesto el ataque de **WannaCry**, que explota vulnerabilidades en el sistema operativo Windows descubiertas y "robadas" a la NSA.

Acopio de vulnerabilidades

El ejecutivo advirtió, en el blog oficial de la compañía tecnológica, que el "acopio" de vulnerabilidades informáticas por parte de los gobiernos se ha convertido en un "patrón emergente" que causa "daños generalizados" cuando la información se filtra.

- **El "accidente" por el que un joven de 22 años se hizo "héroe" al detener el virus que secuestró computadoras en unos 150 países**

Para el ejecutivo de Microsoft, el ciberataque representa un vínculo "imprevisto pero preocupante" entre las que consideró las dos amenazas más serias para la ciberseguridad: **la actuación a nivelestatal y laactuación criminal organizada**, según manifestó.



El ejecutivo de Microsoft urgió a una "acción colectiva" y al trabajo en común del sector tecnológico, los clientes y los gobiernos para generar una mayor protección frente a ciberataques.

Smith comparó el ataque del programa maligno WannaCry al robo de "armas convencionales" al ejército estadounidense para exigir a los gobiernos que cambien sus "métodos" y se adhieran a las "mismas normas" que rigen en el mundo físico.

- **Cómo una fisura en Windows fue el origen del ciberataque de alcance mundial (y por qué muchos culpan a la Agencia Nacional de Seguridad de EE.UU.)**

En este sentido, recordó que el pasado febrero la compañía llamó a renovar la Convención Digital de Ginebra para que sea **un requisitogubernamental "informar de las vulnerabilidades a los proveedores,enlugar de almacenarlas, venderlas o aprovecharlas"**.

El ejecutivo de Microsoft urgió a una "acción colectiva" y al trabajo en común del sector tecnológico, los clientes y los gobiernos para generar una mayor protección frente a ciberataques.

Actualizaciones

La firma tecnológica tiene 3.500 ingenieros de seguridad en su plantilla.

"Hemos estado trabajando a destajo desde el viernes para ayudar a nuestros clientes afectados por el incidente", aseguró el asesor legal, quien destacó los "pasos adicionales" tomados por Microsoft para asistir a sus usuarios con sistemas antiguos de la compañía.

- **Ciberataque masivo a escala global: 5 preguntas para entender qué es y de donde surgió el virus WannaCry**

No obstante, matizó que el hecho de que tantos ordenadores fueran vulnerables al ataque dos meses después de que Microsoft lanzara el "parche" para el fallo demuestra que "**no hay manera de que losclientes se protejan contra las amenazas a menos que actualicen sussistemas**".

Al menos 150 países fueron afectados por el ransomware

El *ransomware* WannaCry, que exige un pago en la moneda digital Bitcoin para recuperar el acceso a los ordenadores, ha golpeado a centros de salud en el Reino Unido, grandes empresas en Francia y España, la red ferroviaria en Alemania, organismos públicos en Rusia y universidades en China, entre otros.

- **Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país**

Un experto informático no identificado del Reino Unido consiguió que el ciberataque quedara inhibido varias horas después de comenzar a causar estragos el viernes, pero advirtió de que nuevas versiones del *malware* se propagarán "con bastante probabilidad el lunes".

Lunes en Asia

El "accidente" por el que un joven de 22 años se hizo "héroe" al detener el virus que secuestró computadoras en unos 150 países

Redacción
BBC Mundo

13 mayo 2017

EPA

El programa malicioso detuvo el funcionamiento de las computadoras en instituciones en unos 150 países. Exigía un pago de $300 en la moneda electrónica Bitcoin para liberar cada equipo.

El ciberataque que golpeó el viernes los sitios de organizaciones en unos 150 países fue muy efectivo, pero tenía un punto débil que vio un analista informático que ahora es considerado un "héroe".

Una simple acción de un joven de 22 años, conocido en internet con el nombre de **MalwareTech**, logró contener parte del *ransomware*, el virus troyano que literalmente secuestra la información de una computadora y exige un pago para liberarla.

- **El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de casi 100 países**
- **"Paga o destruimos tus datos": cuáles son los 'ramsonware' "más buscados" por la policía en Europa**

MalwareTech se encontraba la noche del viernes analizando el código detrás del programa malicioso cuando hizo un descubrimiento que resultaba evidentemente extraño.

El software, llamado **WannaCry**, se estaba esparciendo al usar una extraña dirección de internet, que por seguridad de los lectores no mencionamos, pero notó que esa dirección no llevaba a ningún sitio.

Eso se debía a que **nadie había registrado ese dominio,** es decir, la página base en la red la cual funcionaba como base para esparcir el virus y activar su daño.

PA

El programa malicioso usado en el 'ransomware' exige a contrarreloj un pago por la liberación del sitio.

Al notarlo, MalwareTech pagó los US$10,69 para comprar la dirección web, y al ser el propietario pudo acceder a los datos analísticos y tuvo una idea de cómo estaba funcionando este *ransomware*.

Y no solo eso: al registrar la dirección también **notó que el software malicioso se detuvo**.

"En realidad, en parte fue por accidente", dijo en una charla con la BBC.

Su hallazgo hizo que potenciales víctimas en todo el mundo, tanto instituciones privadas como del gobierno, evitaran perder miles de millones de dólares.

- **Cómo una fisura en Windows fue el origen del ciberataque de alcance mundial (y por qué muchos culpan a la Agencia Nacional de Seguridad de EE.UU.)**

¿Qué pasó?

Desde el viernes, la campaña masiva de *ransomware*, un ataque en el que los perpetradores piden dinero a cambio de liberar el acceso a los sistemas, afectó a instituciones de **Reino Unido, Estados Unidos, China, España, Italia, Vietnam y Taiwán, entre otros, pero principalmente de Rusia**.

¿QUÉ ES UN RANSOMWARE?

Es un software malintencionado que restringe el acceso a algunos archivos y **que pide un rescate a cambio**

Se transmite como un troyano o un gusano capaz de duplicarse.

Se presenta como un programa inofensivo pero suele infectar el sistema operativo explotando una vulnerabilidad del software y cifrando archivos.

Entre los más afectados estuvo el Servicio Nacional de Salud británico, la empresa española Telefónica, el fabricante de vehículos Renault, y la servicio de mensajería de FedEx.

Primero se creía que el virus tenía una especie de "interruptor de apagado" para detener la propagación del *ransomware,*en caso de que las cosas se salieran de su control para su creador.

- **Ciberataque masivo a escala global: 5 preguntas para entender qué es y de donde surgió el virus WannaCry**

Si ese fuera el caso, el acto de registrar la dirección web misteriosa activó ese interruptor.

Pero luego de horas de análisis, "sin pegar un ojo" para dormir, MalwareTech piensa que no era ese el caso, sino **una manera de detectar si el *malware* se estaba ejecutando** en una "máquina virtual".

EPA

El sistema de salud pública británico NHS fue una de las entidades más golpeadas por el 'ransomware' llamado "WannaCry".

Se trata de un software seguro, desechable, que los investigadores utilizan para inspeccionar los virus.

Mientras que un ordenador real no era capaz de acceder a la dirección registrada por el joven de 22 años, **una máquina virtual podía obtener respuesta artificialmente y dar por válido el sitio como real**.

"Mi registro (de la dirección) causó que todas las infecciones a nivel mundial creyeran que estaban dentro de una (máquina virtual) y salieran... por tanto, mi intencional acción previno la propagación y posterior petición de rescate de los ordenadores", describió MalwareTech.

El investigador ha sido llamado un **"héroe accidental"** por frenar la propagación del virus.

"Yo diría que eso es correcto", dijo a la BBC.

EPA

La principal estación de transporte en Frankfurt se vio afectada por el virus, lo que dejó sin funcionamiento las pantallas de salidas y llegadas.

¿El 'ransomware' está derrotado?

Si bien parece haber detenido una cepa de la propagación del virus con el registro de la dirección web, esto **no significa que el *ransomware* en sí haya sido detenido.**

Los archivos que ya fueron enviados por el software malicioso todavía piden un rescate

"Es muy importante que la gente actualice su sistema", planteó MalwareTech, con los parches de seguridad que ofrece Windows para evitar la entrada de este virus

Los expertos en seguridad han advertido que podrían aparecer nuevas variantes de WannaCry que ignoren al "interruptor de apagado".

"Esta variante no debe estar extendiéndose más lejos, sin embargo, **es casi seguro que habrá imitaciones**", dijo el investigador de seguridad Troy Hunt en un blog.

MalwareTech advirtió: "Hemos detenido este, pero habrá otro que venga y no va a poder ser detenido por nosotros".

"Hay una gran cantidad de dinero en esto, no hay ninguna razón para que se detengan. No es mucho esfuerzo para ellos cambiar el código y empezar de nuevo", alertó.

Temas relacionados

Tecnología

Compartir Acerca de compartir

Volver Arriba

Contenido relacionado

El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de unos 150 países
13 mayo 2017

Virus WannaCry: ¿corre peligro mi computadora?
12 mayo 2017

Cómo una fisura en Windows fue el origen del ciberataque de alcance mundial (y por qué muchos culpan a la Agencia de Seguridad Nacional de EE.UU.)
13 mayo 2017

Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país
6 mayo 2017

El mapa global de ciberataques en tiempo real
5 mayo 2017

Principales noticias

"Tienes que ser fuerte, tu hijo está muerto": la conmovedora historia del joven Juan Pablo Pernalete, uno de los casi 40 muertos en las protestas de Venezuela
Elvira y José Gregorio recibieron la dura noticia de que su hijo había fallecido en medio de una de las protestas que acabaron en violencia en Venezuela, donde este lunes se espera una nueva

Microsoft responsabiliza a la Agencia de Seguridad Nacional de EE.UU. de propiciar el ciberataque masivo que afectó al menos a 150 países
15 mayo 2017

14/05/2017 - 08:53 | Clarin.com | Sociedad

Ataques informáticos

El ciberataque ya afectó a 150 países y temen que la cifra aumente mañana

La coordinadora de los policías de Europa espera una nueva oleada cuando el lunes las personas vuelvan al trabajo y enciendan las computadoras.

El mensaje del ataque en una de las pantallas de la estación central de trenes de Frankfurt , Alemania.

Ciberataque

El **ciberataque mundial del viernes dejó 200.000 víctimas** en al menos 150 países informó el director de Europol, Rob Wainwright.

En declaraciones a la cadena británica ITV, Wainwright advirtió de que el virus seguirá propagándose a partir del lunes **"cuando la gente vuelva al trabajo y encienda su computadora a partir del lunes".**

El software malicioso que se propagó el viernes bloqueó los equipos informáticos en numerosos centros de salud en el Reino Unido, así como en empresas y organismos en España, Francia, Alemania y Rusia.

"Llevamos a cabo cerca de 200 operaciones globales al año contra el cibercrimen, pero nunca hemos visto nada como esto", dijo Wainwright.

Mirá también
Cómo se detuvo el ciberataque que afectó a 99 países y grandes corporaciones

El responsable de Europol alertó de que **el sector sanitario está especialmente expuesto a ataques similares,** y recomendó que todas las organizaciones den prioridad a medidas para proteger sus sistemas y actualicen las versiones del software con el que trabajan.

"El reciente ciberataque a gran escala sirve para enviar un mensaje muy claro. Todos los sectores son vulnerables y deben tomarse absolutamente en serio la necesidad de funcionar con sistemas actualizados e instalar todos los parches disponibles", afirmó el director de Europol.

Wainwright también citó a los bancos como un sector de referencia, que ha aprendido a manejar las amenazas cibernéticas. "Muy pocos bancos en Europa, si es que ha habido alguno, han resultado afectados por este ataque, porque han aprendido a partir de la dolorosa experiencia de ser el objetivo número uno para el cibercrimen", sostuvo el funcionario británico.

Mirá también
Las grandes empresas y organizaciones golpeadas por el ciberataque mundial

El responsable del organismo policial europeo indicó que **trabajan con la hipótesis de que el ataque del viernes fue perpetrado por criminales, no por terroristas.**

Las víctimas del ciberataque vieron cómo sus equipos quedaban bloqueados y s**e les pedía un rescate en la moneda digital Bitcoin para poder recuperar sus archivos**.

Microsoft lanzó a las pocas horas del ataque un parche de seguridad, el MS17-010, para su sistema operativo Windows que debería cerrar la brecha por la que se filtró el ataque, por lo que su extensión debería ser frenada.

El virus afecta a computadores que usan el sistema operativo de Microsoft y sus programas más populares como Word o Excel.

La ministra de Interior británica, Amber Rudd, recomendó a los numerosos hospitales y centros de salud afectados en el Reino Unido "no pagar" la cantidad que demandaba el software malicioso

Fuente: EFE