

JOHN MARKOFF 14/03/2009

Hace dos décadas, un brillante estudiante recién licenciado puso a Internet contra las cuerdas con un simple programa informático que saltaba de ordenador en ordenador a la velocidad del rayo, bloqueando completamente la por aquel entonces diminuta red en el transcurso de unas pocas horas. El programa pretendía ser una broma digital. Pero desde entonces las cosas han empeorado considerablemente.

Lo suficiente para que los ingenieros y los expertos en seguridad tengan cada vez más claro que la seguridad y la privacidad en Internet se han vuelto tan exasperantemente esquivas que la única manera de solucionar el problema es volver a empezar.

Las características que debería tener la nueva Internet todavía es algo muy debatido, aunque una de las alternativas sería, de hecho, crear una "comunidad cerrada" en la que los usuarios podrían ceder su anonimato y ciertas libertades a cambio de seguridad. Hoy en día eso es lo que hacen muchos usuarios de Internet pertenecientes a empresas o al Gobierno.

Si se generalizara el uso de una nueva red más segura, la actual Internet podría terminar siendo el barrio conflictivo del ciberespacio. Entrarías en él por tu cuenta y riesgo y no podrías bajar la guardia.

"A menos que nos replanteemos la actual Internet, nos enfrentaremos a una serie de catástrofes públicas", comenta Nick McKeown, un ingeniero de la Universidad de Stanford en California que está involucrado en la construcción de una nueva Internet.

Eso se puso de manifiesto a finales del año pasado, cuando un malintencionado programa que se cree que fue lanzado por una banda criminal del Este de Europa de repente apareció después de haber esquivado con facilidad las mejores ciberdefensas del mundo. Conocido como Conficker, rápidamente infectó más de 12 millones de ordenadores devastando todo a su paso, desde el sistema informático de un quirófano de Inglaterra hasta las redes informáticas del ejército francés.

Una nueva versión del programa conocida como Conficker B++ fue puesta en circulación en febrero después de que los equipos de seguridad inutilizaran la capacidad destructiva del original. Conficker sigue siendo una bomba de relojería. Pero pase lo que pase, Conficker ha demostrado que Internet continúa siendo muy vulnerable a un ataque coordinado.

"Si buscáramos un Pearl Harbor digital, ahora mismo tenemos a los barcos japoneses dirigiéndose en tropel hacia nosotros en el horizonte!", afirma Rick Wesson, director ejecutivo de Support Intelligence, una empresa de asesoría informática.

Los diseñadores originales de Internet nunca previeron que llegaría un día en que la red que habían creado soportaría todas las comunicaciones y el comercio del mundo. Se le prestó poca atención a la seguridad.

"En muchos aspectos probablemente estemos peor que hace 20 años, porque se ha dedicado todo el dinero a poner parches al actual problema en lugar de invertir en rediseñar nuestra infraestructura" opina Eugene Spafford, director ejecutivo del Centro para la Educación e Investigación sobre Garantías y Seguridad de la Información de la Universidad de Purdue, en Indiana, y pionero en la investigación sobre seguridad en Internet.

A pesar de existir una próspera industria de seguridad informática mundial que se espera que alcance los 62.000 millones de euros en ingresos el próximo año, y de que en 2002 el propio Microsoft empezase a intentar mejorar la seguridad de sus programas, la seguridad en Internet sigue deteriorándose.

Hasta las redes militares mejor pertrechadas han demostrado ser vulnerables. En noviembre, el mando militar de EE UU a cargo de las guerras de Irak y Afganistán descubrió que sus redes informáticas habían sido infectadas a propósito con programas que podrían haber permitido un espionaje devastador.

Ésa es la razón por la cual científicos armados con dólares federales para investigación y que trabajan en colaboración con el sector están intentando descifrar cuál es la mejor manera de volver a empezar. En Stanford, donde se diseñaron los protocolos de *software* para la Internet original, los investigadores están creando un sistema que haga posible deslizar desapercibidamente una red más avanzada bajo la Internet actual. A finales de verano

empezará a funcionar en ocho universidades.

La idea es construir una nueva Internet mucho más segura y capaz de soportar una nueva generación de aplicaciones de Internet todavía no inventadas.

El proyecto Clean Slate [Borrón y cuenta nueva] de Stanford proporcionará a los diseñadores de equipos y programas informáticos una serie de herramientas para hacer de las características de seguridad una parte más integral de la red.

Una red más segura implicará, casi con total seguridad, menos anonimato y privacidad. Es probable que ése sea el gran sacrificio que tengan que hacer los diseñadores de la próxima Internet. Pero demostrar la identidad probablemente seguirá siendo extraordinariamente difícil en un mundo en el que resulta tan sencillo entrar en el ordenador de alguien desde el otro lado del mundo.

Mientras eso siga siendo así, construir un sistema completamente fiable continuará siendo prácticamente imposible.