FRANCESC BRACERO Barcelona

e ha acabado salir a la calle para manifestarse? ¿Es internet el nuevo campo de batalla? ¿Está en cuestión el uso de la red por parte de las em-presas si esta las hace vulnerables? El grupo Anonymous, con sus ataques a las webs de firmas importantes, como Mastercard, Visa, PayPal, Twitter, o el banco suizo Post Finance, ha demostrado que el activismo político tiene herramientas para proporcionar, cuando menos, un buen susto y algunas pérdidas a las compañías que han dado la espalda al portal Wikileaks, convertido para ellos en un icono de la libertad frente a gobiernos. La guerra se libra ahora en el ciberespacio.

Esta lucha en internet no es nueva. Durante años, no sólo los activistas políticos, sino también mafias y terroristas, han puesto su vista en la red como escenario preferente para sus movimientos. El motivo es sencillo. Como explica Luis Corrons, director técnico de PandaLabs (empresa de software de seguridad), "internet no tiene fronteras. Los delincuentes lo saben y se aprovechan de ello. La policía que investiga un delito se encuentra al final con barreras que no puede saltar, que son las fronteras físicas entre países". Las investigaciones internacionales, debido a los mecanismos burocráticos, se convierten en muchas ocasiones en un sistema "poco efectivo y muy lento" ante las actuaciones delictivas.

Así que moverse en la red también puede ser mucho más eficaz que salir a la calle detrás de una pancarta y un megáfono. Corrons señala que la diferencia entre los ataques DDOS (de denegación de servicio) a webs que se han producido en otras ocasiones y los de ahora parece estar sólo en "la motivación" y no en los instrumentos que emplean. "No hablaría de ciberguerra -objeta-, sino de ciberprotesta. Se trata de gente que voluntariamente realiza una serie de acciones tratando de defender lo que sea".

En toda la polémica de las últi-

En toda la polémica de las últimas semanas, la propia Wikileaks ha sufrido ataques, pero han surLas acciones de activistas de la red para vengar a Wikileaks revelan un internet inseguro para las empresas

# GUERRA en la nube

gido sus "vengadores". Un grupo llamado Anonymous ha promovido ataques directos contra las webs de quienes han rechazado colaborar con el portal de Julian Assange o quienes se le han opuesto de forma frontal, como los senadores Joe Lieberman y Sarah Palin.

Un ataque DDoS consiste en provocar la caída de una página

#### SIN LÍMITES

La protesta aprovecha la falta de límites de la red en un mundo real que sí tiene fronteras

## Las empresas de seguridad abogan por armonizar leyes y crear una autoridad

web mediante la saturación de peticiones simultáneas que sobrepasa su capacidad para atenderlas. Así han caído páginas como las de Mastercard o Visa que, al ser compañías importantes que fían parte de su actividad en internet, tenían mecanismos de defensa que, no obstante, no han podido evitarles daños.

Anonymous llama a su actuación Operación vengar a Assange. En su web aparece el siguiente mensaje: "Se ha iniciado la primera ciberguerra seria. El campo de batalla es Wikileaks. Vosotros sois las tropas". Es un mensaje en Twitter de John Perry Barlow, antiguo letrista del grupo musical Grateful Dead v vicepresidente de la Electronic Frontier Foundation, una fundación dedicada a los derechos digitales. Perry ya se ha desmarcado del uso que han hecho de su proclama, al señalar a la agencia Reuters que apoya la libertad de expresión y, por tanto, reniega de los ataques DDoS. El presidente de la Asociación

de Internautas, Víctor Domingo, opina que estas situaciones se originan por la falta de mecanismos de justicia rápidos adecuados a las características de internet. Domingo, favorable a la publicación de los documentos públicos de Wikileaks, considera que el marco legal tendría que evitar "que nadie, gobiernos o activistas, tenga la posibilidad de atajos. Todo esta sucediendo porque la justicia no es todo lo rápida que debería ser". Domingo apunta que "todos los agentes sociales están usando internet en la medida de sus posibilidades, no es ni más ni menos que un reflejo de la sociedad". El presidente de la Asociación de Internautas cree que la gran batalla en internet está en los intentos de crear "una in-ternet de primera y otra de segunda. Una segura y funcional, y otra en la que esté toda la basura. Es lo que se intenta mientras que muchos queremos que sea accesible, y universal. Esa es la batalla de la neutra-lidad"

Una posible armonización de las legislaciones de los países en materia de internet se presenta dificil, porque algunos de los comportamientos que son delito en unos países no lo son en otros, aunque la

idea de algún tipo de regulador neutral en la red es algo que reclaman muchos.

El experto belga Eddy Willems, que es actualmente "evangelista" de seguridad de la compañía alemana de software de seguridad G Data, considera que "definitivamente existe la necesidad
de una mayor discusión de nivel
internacional para, en primer lugar, organizar mejor las leyes,
puesto que hay muchas diferencias entre ellas".

También el director técnico de PandaLabs se pronuncia a favor de mecanismos de control internacionales. "Con un organismo supranacional que tuviera competencias y pudiera investigar todos los delitos en internet, a to-

### CIBERATACANTE

#### Un joven holandés, detenido

In adolescente de 16

años fue detenido e interrogado por la policia
judicial holandesa la madrugada de ayer en La

Haya por haber participado en los ciberataques de
los simpatizantes de

Wikileaks contra las páginas web de Mastercard y
Visa. El joven será puesto hoy a disposición de

un juez de Rotterdam
para responder de ello.

# Ataques cibernéticos

El grupo Anonymous ha lanzado ataques DDoS contra proveedores que se han negado a dar servicio a Wikileaks. Se han registrado ataques a cinco empresas o instituciones. El DDoS (Denegación de Servicios Distribuidos) consiste en lanzar numerosas peticiones a un servidor que aloja una página web de forma que el servicio de hosting no lo soporta.

Anonymous (anónimo) ha reivindicado un ataque contra las páginas web de Mastercard y Visa en represalia por la decisión de retirar los servicios que prestaba al portal Wikileaks. Los mismos hackers son responsables del ataque a la Fiscalía sueca, que ha presentado los cargos por abusos sexuales contra Julian Assange, y estuvo todo un día caída.







MENSAIES DE APOVO DESDE **ANONYMOUS** 

"Protesta, informa interroga, lucha". El futuro de internet pende de la balanza"

#### **Alternativas**

"Facebook y otras redes sociales son sitios de crítica a la distribución de la información"

#### Un referente

"Ahora tenemos la oportunidad de dar nuestro apovo a Wikileaks. Nosotros podemos evitar un futuro más opresivo" Por Assange

"Vota a Julian como personaje del año 2010 en 'The Times



dos nos iría mucho mejor", considera Luis Corrons.

PandaLabs ha monitorizado los ataques DDos lanzados por Anonymous. La protesta se ha basado en pedir a la gente que quería colaborar con este grupo que se descargara una aplicación lla-mada LOIC (siglas de Low Orbit Ion Cannon -cañón de iones de baja órbita-) que permitía lanzar el ataque. Según los expertos, va-rios cientos de miles de personas participaron en la operación.

Este tipo de comportamiento, que se ha coordinado mediante la utilización de los micromensajes de Twitter, lleva la protesta social a una nueva frontera.

Corrons prevé que la protesta en favor de Wikileaks va a seguir: ACCIÓN MASIVA Cientos de miles de personas han actuado de forma voluntaria en los ciberataques

PORVENIR INCIERTO Los expertos auguran un internet con más problemas de crimen y terrorismo

"Creen que lo que están haciendo es completamente justo. Ellos van a responder. Están defen-diendo la libertad". Pero estas acciones, que dejan

indefensas a las empresas, revelan un aspecto de internet preocupante: la seguridad. Los expertos auguran que el internet del futuro, será más inseguro. "Desafortunadamente, si -afirma Willems-, claro que es difícil predecirlo, pero internet son las calles virtuales del futuro y eso nos lleva automáticamente a más problemas criminales y de terrorismo. Los crímenes parecen moverse en esa dirección, mientras que los cibercriminales son más difíciles de seguir comparados con el mundo real".

# Un asedio en internet con un 'cañón de iones'

En algún ataque se han usado ordenadores infectados con virus

F. BRACERO Barcelona

a diferencia entre los ataques de las mafias criminales y los de los activistas contra las páginas web está en su finali-dad. Mientras los primeros extorsionan a las compañías al estilo de las bandas mafiosas que ofrecen "protección" -o ausencia de ataques- a cambio de un pago económico, en el segundo caso se trata de protestas sociales. Anonymous, que es el grupo que ha organizado los ata-ques pro Wikileaks, ya protagonizó en octubre un ciberataque del mismo estilo contra las webs del Ministerio de Cultura y la Sociedad General de Autores y Editores (SGAE). En aquella ocasión, se trató

de una serie de ataques coordinados bajo el epígrafe de Operation Payback a varias páginas webs de todo el mundo relacionadas con la industria de gestión de derechos de autor.

En los ataques de ahora contra Mastercard y Visa, se ha uti-lizado una aplicación llamada LOIC (siglas en inglés de cañón de iones de baja órbita). Este programa suele utilizarse, paradójicamente, para probar la resistencia de una página web a los ataques DDoS. Según Eddy Willems, de G Data, "si apuntas con esto a alguien más, el efecto puede ser bastante dañino".

Así que unos cientos de miles de personas que sintonizaron con la idea de Anonymous apuntaron a las páginas de sus víctimas con el programa LOIC y, simplemente, "dispararon". La organización de estas acciones sigue un esquema de democracia asamblearia. Si las páginas atacadas hubieran utilizado un sistema de prevención de intrusiones podrían haber ralentizado el ataque, aunque todo apunta a que no fue así.

En el caso del ataque a Payal, según constató Willems, se utilizó un botnet, un tipo de virus que hace que los ordenadores que han sido infectados participen en el ataque sin conocimiento ni autorización por parte de sus dueños. Unas 30.000 máquinas infectadas participaron en esta acción.

Los datos coinciden con los de la investigación de PandaLabs, que constató que algunos de

El programa usado para la protesta está pensado para probar la resistencia de una web contra ataques

los que se unía a la protesta te-nían su propia red de botnets y los puso al servicio de la protesta. La propia empresa de soft-ware de seguridad sufrió un pequeño ataque el miércoles.

Contra estos ataques hay pocas defensas mágicas. Los expertos recomiendan una serie de protecciones en las partes más vulnerables del negocio de internet. El problema es que protegerse contra un ataque masivo acaba saliendo caro. En el verano del 2009, Google y Twitter fueron atacadas desde Georgia. Sólo el primero resistió.

El ataque a PayPal, por dejar de gestionar la transferencia de donaciones a Wikileaks, supuso ocho horas de interrupción del sitio web y los servicios del popular sistema de pago.

En el caso de PostFinance, los usuarios de la entidad han llegado a pedir a través de Twitter a los ciberactivistas que pararan al menos diez minutos para poder utilizar los servicios on line. Otra de las empresas atacadas ahora desde Anonymus ha sido Amazon por la actitud de la compañía que ha rechazado los servicios de hosting a WikiLeaks. Y ha amenazado a Twitter.

El propio sitio web de Anonymous, donde informa periódicamente de sus planes de ataque, ha caído también víctima de un ataque DDoS que lo dejó inactivo durante varias horas.







