



¿Se puede apagar Internet?

En febrero del año 2000 se utilizó una red Trin00 para realizar un ataque DDoS contra máquinas de Yahoo, Amazon y Ebay. Desde entonces, esta técnica se fue desarrollando y alcanzó su madurez el mes de mayo de 2007 cuando se utilizó contra el estado de Estonia. Sin embargo, no ha sido hasta la aparición de Anonymous y su guerra contra la Cienciología cuando los DDoS se hacen realmente famosos. Incluso se ha llegado a proponer "Apagar Internet" utilizando estas técnicas, pero no está muy claro que pueda ser así; sin embargo, la pregunta es legítima: ¿es ello posible?

El 12 de febrero de 2012 un comunicado¹, colgado en el **pastebin.com** y supuestamente firmado por Anonymous, amenazó con atacar a los servidores raíz del sistema de resolución de nombres en Internet durante el día 31 de marzo de 2012. A esta operación la bautizaron como "Operation Global Blackout 2012" y los motivos alegados en ella son "protestar contra la iniciativa americana SOPA², ir contra Wall Street, contra los políticos irresponsables y contra los banqueros que están dejando al mundo famélico para satisfacer sus propias necesidades y, además, por pura diversión".

La idea es apagar Internet pero aclaran que esta acción es simplemente una protesta, que no intentar cargarse Internet, sino apagarla temporalmente en "aquellas zonas que hagan más daño". Los promotores anuncian que el efecto puede durar horas o incluso algunos días, pero que, independientemente de ello, será "global". La idea es tumbar los trece servidores básicos que constituyen el núcleo del sistema de direcciones³ de la Internet que hoy co-

nocemos. La anulación de ese sistema de conversión entre nombres de dominio y direcciones IP, retrotraería la red a antes de 1987.

El sistema DNS tiene una estructura jerárquica y arborescente, en la que las hojas y los nodos del árbol son componentes de los nombres de dominio. Cada uno de esos nombres consiste en la concatenación de todas las etiquetas que hay en el camino desde la raíz del sis-

tema hasta la dirección IP a la que representa. El sistema de resolución de nombres de dominio es una estructura esencialmente distribuida en la que se ve involucrado un enorme número de máquinas. Además de eso, su funcionamiento incluye el uso intensivo de cachés, por lo que en él los cambios se propagan lentamente y requieren del orden de dos días para consolidarse.

La posibilidad de que cayese el sistema DNS ya se anunció en 2002 y, de hecho, ya se realizaron varios ataques con éxito en 2002 y 2007. El ataque del 21 de

ya que, en abril de 1997 y por problemas técnicos⁵, se cayeron las siete raíces que tenía entonces el sistema. El ataque del 6 de febrero de 2007 empezó a las 10 am y duró veinticuatro horas. En este caso cayeron dos servidores raíz y otros dos sufrieron un tráfico muy intenso que supieron disipar redirigiéndolo a otros servidores⁶. Lo peculiar de este incidente es que se hicieron declaraciones⁷ desmesu-



Es sorprendente también cómo se puede secuestrar el tráfico de enormes porciones de la Red, para llevarlo por donde no estaba pensado hacerlo pasar. Eso fue lo que ocurrió en el incidente de noviembre de 2010 en el que, durante 18 minutos, todo el correo electrónico de los EE.UU. pasó (en claro) a través de servidores propiedad del gobierno chino.

tema hasta la dirección IP a la que representa. El sistema de resolución de nombres de dominio es una estructura esencialmente distribuida

octubre de 2002 duró una hora y afectó a los 13 servidores raíz del sistema⁴. En realidad, ese fue el segundo gran fallo de esa instalación

radar que clamaban para que los EE.UU. considerasen "lanzar un contrataque o bombardear la fuente del ciberataque". Estas salidas

¹ Ver <http://pastebin.com/NKbnh8q8>

² Ver http://es.wikipedia.org/wiki/Stop_Online_Piracy_Act

³ Ver <http://es.wikipedia.org/wiki/DNS>

⁴ Ver <http://www.isc.org/f-root-denial-of-service-21-oct-2002>

⁵ Ver http://news.cnet.com/Router-glitch-cuts-Net-access/2100-1033_3-279235.html

⁶ Ver http://icann.org/announcements/factsheet-dns-attack-08mar07_v1.1.pdf

⁷ Ver <http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html>

de tono, sin duda, dieron preeminencia a unos ataques cuya efectividad había dejado mucho que desear.

Así pues, atacar a una estructura de este tipo no parece tarea fácil y su éxito es poco probable. Es extraño que el colectivo Anonymous realmente se quiera embarcar en una guerra tan pírrica como esta⁸. Aunque es difícil hablar de confirmaciones y negaciones de una organización sin dirigentes ni estructura, lo cierto es que Anonymous ha negado en Twitter⁹ que la operación Global Blackout sea real y se ha referido a ella como otro engaño similar al de #OpFacebook, que pretendía tumbar Facebook el 5 de noviembre de 2011.

TCP/IP se diseñaron para evitar que hubiese nodos críticos cuya destrucción pudiese acarrear la denegación del servicio. Sin embargo, **Internet puede apagarse y ya se han dado algunos casos de ello.**

Poco después de medianoche del 28 de enero de 2011, el gobierno egipcio,



Puede que sea difícil apagar Internet a nivel planetario, pero resulta sorprendentemente sencillo hacerlo a nivel local.

a la vista de los tres días anteriores de protestas contra el régimen y organizadas en parte a través de Facebook y otras redes sociales,

A las 00:40 am la operación estaba completa y el 93% de la Internet Egipcia era inaccesible. Al día siguiente los manifestantes debieron ir a la Plaza de Tahrir en una completa "oscuridad digital", y aun así Mubarak terminó perdiendo el poder. Sin embargo, debemos aprender una lección importante

sobre la vulnerabilidad real de Internet y sobre la existencia evidente de un control de arriba hacia abajo, lo que va en contra de las

como alternativa a la clásica comunicación a través de circuitos. Puede que sea difícil apagar Internet a nivel planetario, pero **resulta sorprendentemente sencillo hacerlo a nivel local.** También es sorprendente cómo se puede secuestrar el tráfico de enormes porciones de la Red, para llevarlo por donde no estaba pensado hacerlo pasar¹¹. Eso fue lo que ocurrió en el incidente de noviembre de 2010 en el que, durante 18 minutos, todo el correo electrónico de los EE.UU. pasó (en claro) a través de servidores propiedad del gobierno chino¹².

A fin de cuentas, Internet circula por los cables¹³ de fibra óptica que unen los continentes, pero no son tantos como para asegurar una redundancia suficientemente alta que impida su bloqueo y control. Ya en la primera guerra mundial, británicos y alemanes intentaron sistemáticamente destruir las redes de comunicaciones del otro bando cortando cables submarinos utilizando barcos y submarinos¹⁴. Durante la Guerra Fría, la Armada de los EE.UU. y la NSA consiguieron colocar sensores que les permitían interceptar, debajo del agua, las líneas de comunicación soviéticas en la que se conoce como Operation Ivy Bells¹⁵.

Aunque la red de cables de fibra óptica fuese suficiente redundante como para asegurar que nadie pudiese quedarse aislado, la situación es muy diferente dentro de los países, donde **unas pocas manos controlan todos los nodos que prestan el servicio,** y

Solo cuando se instalen redes realmente distribuidas para conectar a los usuarios, y solo entonces, Internet será resistente a la censura, a la manipulación, al control, al espionaje, a los sectarismos y, de paso, a los ataques DDoS.

Independientemente de la propuesta de tumbar los DNS, lo que sí podemos preguntarnos es si se puede "apagar Internet". Ante esta cuestión, casi todo el mundo se remitirá a los orígenes de Internet como un proyecto del DARPA norteamericano y se resaltarán que, precisamente, los protocolos

decidió "apagar Internet". Al parecer bastaron cinco llamadas telefónicas dirigidas a los cinco ISPs más importantes del país. A las 00:12 am, hora del Cairo, el ISP Telecom Egypt empezó a apagar las conexiones con sus clientes y, en menos de trece minutos, le siguieron otros cuatro proveedores.

muy cacareadas habilidades de la estructura de Internet para, precisamente, resistir ese control.

Realmente la Internet de hoy no es como nos cuentan muchos al desempolvar los paradigmas que Leonard Kleinrock publicó en julio de 1961 sobre la teoría de conmutación de paquetes¹⁰

⁸ Ver <http://erratasec.blogspot.com/2012/02/no-anonymous-cant-ddos-root-dns-servers.html>

⁹ Ver <https://twitter.com/#!/YourAnonNews/status/170243270801231872>

¹⁰ Ver http://en.wikipedia.org/wiki/Packet_switching

¹¹ Ver "The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America" de James Bamford, Ed. Doubleday 1ª Ed Octubre de, 2008. ISBN-13: 978-0385521321

¹² Ver "Report sounds alarm on China's rerouting of U.S. Internet traffic" en <http://goo.gl/8TyhT>

¹³ Ver http://en.wikipedia.org/wiki/List_of_international_submarine_communications_cables

¹⁴ Ver "Nexus: Strategic Communications and American Security in World War I" de Jonathan Reed Winkler, Harvard University Press, June 2008 ISBN-13: 978-0674028395

¹⁵ Ver http://en.wikipedia.org/wiki/Operation_Ivy_Bells

la geometría en la que se incluye al usuario final es de marcado carácter centralista. Manifestación directa de esta realidad la tenemos en **la posibilidad de establecer una censura**¹⁶ férrea en países como China, Irán, Corea del Norte, Arabia Saudí y Siria, o con una **"Internet vigilada"** como es el caso de EE.UU., Australia, la Unión Europea, Rusia, Bahrain, Corea del Sur y los Emiratos Árabes Unidos, por poner algunos ejemplos¹⁷.

A diferencia de lo que perseguía el DARPA a mediados del siglo pasado, la red actual está controlada por un número reducido de nodos que, **por sus ubicaciones estratégicas, se convierten en objetivos naturales de alguien que quiera "apagar Internet"** en amplias zonas del globo o a escala nacional.

Si Anonymous tuviese realmente interés en apagar algo, su objetivo no serían los servidores raíz de los DNS, sino las instalaciones de los ISPs que controlan cada zona de Internet. La mera existencia de nodos excesivamente relevantes es la fuente de la inseguridad de la Red frente a los ataques por denegación de servicio. Solo cuando se instalen redes realmente distribuidas para conectar a los usuarios, **y solo entonces, Internet será resistente a la**

censura, a la manipulación, al control, al espionaje, a los sectarismos y, de paso, a los ataques DDoS.

No hay que olvidar que, además de los ataques DDoS basados en herramientas LOIC¹⁸, la iniciativa **Stop Online Piracy Act (SOPA)**¹⁹ de la administración norteamericana, fue capaz, ella sola, de **mantener apagados** el 18 de enero de 2012, **y durante doce horas más de 7.000 sitios web**²⁰ como Reddit, Wikipedia, Google Mozilla, World-preset alter. Sitios

gicas para comprender este fenómeno. Anonymous es una forma más de "hactivismo" que pretende realizar acciones sociales mediante la **utilización no-violenta de herramientas digitales** ilegales o legalmente ambiguas, y su ámbito de actuación es la desfiguración de webs, las redirecciones, los ataques de denegación de servicio, las parodias y la confección de muchos comunicados (en Twitter y Youtube) con una audiencia que quizás

tente que representa la bolsa de Wall Street y el 1% de la población, o en la **Operación Mayhem**²³ para revitalizar la filosofía básica que dio la luz a WikiLeaks. Para Anonymous, Internet es esencial, es su caldo de cultivo.

Aparte de esos fenómenos sociológicos, el delito contra instalaciones en Internet para la obtención de informaciones valiosas en los diferentes mercados negros de este planeta es algo que seguirá siendo



Si Anonymous tuviese realmente interés en apagar algo, su objetivo no serían los servidores raíz de los DNS, sino las instalaciones de los ISPs que controlan cada zona de Internet. La mera existencia de nodos excesivamente relevantes es la fuente de la inseguridad de la Red frente a los ataques por denegación de servicio.

todos ellos emblemáticos de lo que hoy llamamos Internet.

En realidad, los ataques DDoS se parecen mucho a una **"kedada"** en la que muchos ciudadanos se reuniesen a mirar un escaparate en el que, realmente, les da igual lo que haya. **Los ataques DDoS son una expresión tecnológica del "derecho de manifestación" de los usuarios conectados a Internet**, y, por ello, hay que atender a razones socioló-

no sea despreciable. El **hacktivismo** generalmente solo promueve políticas tales como la libertad de expresión, los derechos humanos, la ética de la información y la desobediencia civil.

Para entender que Anonymous no tiene ningún interés en apagar Internet basta con atender a las razones que esgrime en sus invitaciones a participar con ellos²¹, o en la convocatoria de la **Operación Icarus**²² contra el poder omnipo-

habitual y cotidiano. Sin embargo, esta certeza no puede justificar hablar de ciber guerras, ciberarmas, ciberconflictos o cualquier otra cibertransliteración de los escenarios militares al mundo Internet. **El problema de Internet no está en las reacciones sino en la (falta) de previsión.** No hay que olvidar que, hasta el momento, los ataques y atacantes mas sonados **lo único que han hecho es entrar por las puertas que inadvertidamente les hemos dejado abiertas.** ■

¹⁶Ver http://en.wikipedia.org/wiki/Internet_censorship

¹⁷Ver http://march12.rsf.org/i/Internet_Enemies.pdf

¹⁸Ver http://es.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

¹⁹Ver **"SOPA: Washington Vs. The Web"** en <http://goo.gl/l3NNh>

²⁰Ver <http://sopastrike.com/>

²¹Ver "JOIN US. Anonymous 2012" <http://youtu.be/77avYP2vg4Y>

²²Ver "Operación Icarus 21 de diciembre del 2012" en <http://youtu.be/Afablhvhd2I>

²³Ver "Anonymous 2012 Proyecto Mayhen" en <http://youtu.be/EATyZMo11Y>, nombre extraído de [http://es.wikipedia.org/wiki/Fight_Club_\(novela\)](http://es.wikipedia.org/wiki/Fight_Club_(novela))

JORGE DÁVILA MURO
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad
de Informática – UPM
jdavila@fi.upm.es