Informe *especial* del Consejo
nº 83 de noviembre de 2018

Cero botnets

fiutldtng o Glohol £@ort to *Limpiar Internet*

Jason Healey y Robert K. Knake

COUNCIL on FOREIGN RELATIONS

Informe especial del Consejo
nº 83 de noviembre de 2018

Cero botnets

Construir un esfuerzo global para Limpiar Internet

Jason Healey y Robert K. Knake

El Council on Foreign Relations (CFR) es una organización independiente y no partidista, un grupo de reflexión y una editorial que se dedica a ser un recurso para sus miembros, funcionarios del gobierno, ejecutivos de empresas, periodistas, educadores y estudiantes, líderes cívicos y religiosos y otros ciudadanos interesados, con el fin de ayudarles a entender mejor el mundo y las opciones de política exterior a las que se enfrentan Estados Unidos y otros países. Fundado en 1921, el CFR lleva a cabo su misión manteniendo una membresía diversa, con programas especiales para promover el interés y desarrollar la experiencia en la próxima generación de líderes de la política exterior; convocando reuniones en su sede de Nueva York y en Washington, DC, y otras ciudades donde altos funcionarios del gobierno, miembros del Congreso, líderes mundiales y pensadores prominentes se reúnen con los miembros del Consejo para discutir y debatir los principales temas internacionales; Apoyar un Programa de Estudios que fomente la investigación independiente, permitiendo a los académicos del CFR elaborar artículos, informes y libros y celebrar mesas redondas que analicen cuestiones de política exterior y formulen recomendaciones políticas concretas; publicar *Foreign Affairs*, la revista preeminente sobre asuntos internacionales y política exterior de EE.UU.; patrocinar la revista Independent La publicación de Foreign Affairs, la revista más importante sobre asuntos internacionales y política exterior de Estados Unidos; el patrocinio de grupos de trabajo independientes que elaboran informes con conclusiones y recomendaciones políticas sobre los temas más importantes de la política exterior; y el suministro de información y análisis actualizados sobre los acontecimientos mundiales y la política exterior estadounidense en su sitio web, CFR.org.

El Council on Foreign Relations no adopta ninguna posición institucional sobre cuestiones políticas y no está afiliado al gobierno de Estados Unidos. Todas las opiniones expresadas en sus publicaciones y en su sitio web son responsabilidad exclusiva del autor o autores.

Los Informes Especiales del Consejo (IRC) son informes políticos concisos, elaborados para dar una respuesta rápida a una crisis en desarrollo o contribuir a la comprensión del público de los dilemas políticos actuales. Los informes especiales del Consejo son redactados por autores individuales -que pueden ser becarios del CFR o expertos reconocidos de fuera de la institución- en consulta con un comité consultivo, y su duración prevista es de sesenta días desde su inicio hasta su publicación. El comité sirve de caja de resonancia y proporciona información sobre el borrador del informe. Suele reunirse dos veces, una antes de redactar el borrador y otra cuando se dispone de un borrador para su revisión; sin embargo, a los miembros del comité asesor, a diferencia de los miembros del Grupo de Trabajo, no se les pide que firmen el informe ni que lo aprueben de otro modo. Una vez publicados, los informes se publican en CFR.org.

Para más información sobre el CFR o este Informe Especial, escriba al Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, o llame a la oficina de comunicaciones al 212.434.9888. Visite nuestro sitio web, CFR.org.

Para enviar una carta en respuesta a un informe especial del Consejo para su publicación en nuestro sitio web, CFR.org, puede enviar un correo electrónico a publications@cfr.org. También puede enviarnos las cartas por correo a Publications Department, Council on Foreign Relations, 58 East 68th Street, New York, NY 10065. Las cartas deben incluir el nombre del autor, su dirección postal y su número de teléfono durante el día. Las cartas pueden ser editadas por su longitud y claridad, y pueden ser publicadas en línea. Por favor, no envíe archivos adjuntos. Todas las cartas pasan a ser propiedad del Council on Foreign Relations y no serán devueltas. Lamentamos que, debido al volumen de correspondencia, no podamos responder a todas las cartas.

Este informe está impreso en papel con certificación de cadena de custodia FSC ® por una imprenta certificada por BM TRADA North America Inc.

CONTENIDO

PRÓLOGO

El ciberespacio se parece cada vez más al viejo Oeste americano, sin un verdadero sheriff y con los botnets como forajidos armados. Las botnets, o grupos de ordenadores infectados con software malicioso que se controlan como una sola red, permiten gran parte de la ciberdelincuencia en Internet. Lo hacen permitiendo a quienes controlan la red aprovechar la potencia de la supercomputación para fines nefastos. Las redes de bots se utilizan para difundir spam, enviar correos electrónicos de suplantación de identidad, adivinar contraseñas, romper el cifrado y lanzar ataques distribuidos de denegación de servicio. A pesar de los esfuerzos realizados para eliminar las redes de bots, su número sigue aumentando.

Como sostienen Jason Healey y Robert K. Knake en este nuevo Informe Especial del Consejo, la idea convencional de que las botnets son un problema que hay que gestionar apunta demasiado bajo. Los botnets pueden causar graves daños al permitir a los gobiernos extranjeros reprimir la libertad de expresión en el extranjero y permitirles cerrar las redes nacionales de los países o incluso Internet a nivel mundial. Además, es probable que el daño económico que causan los botnets aumente significativamente con el tiempo a medida que aumente el número de dispositivos conectados a Internet. Por ello, los responsables políticos deberían aumentar su ambición y tratar de librar al mundo de las redes de bots. Aunque tener cero botnets puede ser imposible, los autores concluyen que es necesario establecer un objetivo tan ambicioso para centrar la política.

Los autores proponen varias prescripciones políticas innovadoras. Sugieren que los responsables políticos trabajen para establecer el principio de que los estados son responsables del daño que las redes de bots basadas en sus fronteras causan a otros. Los proveedores de servicios de Internet deberían responsabilizarse mutuamente del tráfico nocivo que sale de sus redes. Deben introducirse incentivos para que los fabricantes

de dispositivos conectados a Internet tomen medidas para asegurar sus dispositivos. Componentes del ecosistema de Internet que son utilizados por los botnets deben ser presionados para que se vigilen a sí mismos y eviten que sus servicios se utilicen con fines delictivos. Por último, si estas medidas no consiguen frenar su crecimiento, puede ser necesario un esfuerzo internacional para acabar con las redes de bots.

La prevalencia de los botnets y los problemas que causan son una prueba más de que muchos de los retos del siglo XXI no pueden contenerse dentro de las fronteras ni abordarse a nivel nacional. En cambio, para minimizar la capacidad de las botnets de hacer daño, los países deberían aplicar el concepto de obligación soberana, o la noción de que los estados soberanos no sólo tienen derechos sino también obligaciones con respecto a otros países. Los gobiernos tendrían la obligación no sólo de evitar la realización de actividades prohibidas, sino también de hacer todo lo que esté en su mano para impedir que otras partes realicen esas actividades desde su territorio. Si los países asumieran esas responsabilidades, el mundo se acercaría al objetivo de cero botnets, algo que interesaría a cualquier entidad con una agenda benigna.

Richard N. Haass
Presidente
Consejo de Relaciones
Exteriores noviembre DE 2018

AGRADECIMIENTOS

Nos gustaría dar las gracias a nuestro comité asesor por compartir sus décadas de experiencia. Aunque somos responsables del contenido y las recomendaciones de este informe, muchas de las ideas y fuentes fueron presentadas por primera vez por los miembros del comité asesor. Spamhaus proporcionó un acceso inestimable a sus datos sobre redes de bots, y Justin Haner, de la Universidad de North-East, les dio sentido. También queremos dar las gracias a Matt Carothers y Gabriel Ramsey por aportar sus profundas perspectivas y experiencia.

Jason Healey y Robert K. Knake

INTRODUCCIÓN

Las redes de bots son la perdición de Internet. Los delincuentes utilizan estos grupos de ordenadores infectados con software malicioso para propagar el spam, enviar correos electrónicos de suplantación de identidad, adivinar contraseñas, hacerse pasar por usuarios y romper el cifrado. Sin embargo, su uso más pernicioso es llevar a cabo ataques de denegación de servicio distribuidos (DDoS). Los ataques DDoS aprovechan el poder de los ordenadores individuales que componen la red de bots para enviar tráfico de Internet a un objetivo, bloqueando así el tráfico legítimo. Hasta el 30% de todo el tráfico de Internet puede atribuirse a las redes de bots, y la mayor parte de ese tráfico procede de ataques DDoS. [1]

La mayoría de los ataques DDoS son de naturaleza delictiva, a menudo utilizados por las empresas para derribar los sitios web o servidores de sus competidores; sin embargo, China, Rusia e Irán han aprovechado las redes de bots con fines geopolíticos. China ha llevado a cabo ataques DDoS contra el *New York Times*, el Falun Gong y las iglesias cristianas chinas en Estados Unidos. Rusia llevó a cabo ataques DDoS a través de proxies contra Estonia en 2007, tras la retirada de una estatua que conmemoraba a los soldados rusos en Tallin, y en 2008, en relación con las operaciones militares rusas contra Georgia. Irán llevó a cabo una serie de ataques sostenidos y a gran escala contra el sector financiero estadounidense entre 2011 y 2013 en respuesta a las supuestas medidas de Estados Unidos contra su programa nuclear. Al parecer, estos ataques costaron a algunos bancos más de 20 millones de dólares al mes para mantener sus sitios web disponibles para los clientes.

La opinión generalizada es que las redes de bots y los problemas que generan deben ser "gestionados"; que las redes de bots y los daños que causan son, aunque un problema, simplemente parte de una Internet abierta y global. Por tanto, las intervenciones para reducir las infecciones de botnets acabarán perjudicando la vitalidad de Internet, perjudicando la

innovación y ahogando la libertad. Esta opinión es errónea por tres razones.

En primer lugar, no se toma en serio el daño a la sociedad que se crea cuando los gobiernos extranjeros atacan directamente las libertades protegidas sofocando la libertad de expresión en Estados Unidos. El hecho de que el gobierno estadounidense haya parecido impotente para hacer algo para detenerlos debería ser motivo de gran preocupación. Cuando el sitio web del periodista especializado en tecnología Brian Krebs quedó fuera de línea por un ataque DDoS, Krebs sólo pudo volver a poner su sitio web en línea cuando Google se hizo cargo y absorbió el ataque a través de su programa Project Shield. [2] Confiar en una empresa privada con ánimo de lucro para proteger la libertad de expresión en Estados Unidos, y en todo el mundo, suscita preocupación.

En segundo lugar, un actor motivado de un Estado-nación podría aprovechar fácilmente millones de sistemas para cerrar las redes nacionales de los países o apuntar a la infraestructura central de Internet y apagar Internet a nivel mundial. Para los gobiernos extranjeros, existen ciertamente escenarios en los que podrían juzgar que tales acciones son ventajosas.

Por último, aunque los daños económicos pueden ser manejables hoy, probablemente no lo serán mañana. La ciberdelincuencia actual puede costar a la economía mundial 600.000 millones de dólares al año, gran parte de los cuales están relacionados con las redes de bots, y estas pérdidas no harán más que aumentar. [3] El Internet de las cosas (IoT) está provocando un crecimiento masivo del número de dispositivos conectados a Internet. Estos dispositivos a menudo no se construyen teniendo en cuenta la seguridad y rara vez se actualizan una vez instalados, lo que da lugar a vulnerabilidades conocidas que pueden ser explotadas por los adversarios, pero que es poco probable que se parcheen. Por lo tanto, es más probable que sean vulnerables a la toma de control como parte de una red de bots, y es menos probable que la infección sea descubierta y remediada. En 2016, la red de bots Mirai dejó fuera de servicio al proveedor de servicios de nombres de dominio Dyn y a muchos de sus clientes, como Airbnb, Amazon, GitHub, HBO, Netflix, PayPal y Twitter. Los delincuentes llevaron a cabo el ataque con solo una fracción de los bots que tenían bajo su control.

Aprovechar incluso un pequeño porcentaje de dispositivos IoT vulnerables daría a un actor malicioso la capacidad de inundar Internet con tráfico que podría interrumpir las funciones principales. A medida que los tres mil millones de personas restantes que aún no están en Internet se conecten, es probable que los índices de infección de los dispositivos IoT de estos usuarios sean elevados. En la actualidad hay unos dieciséis mil millones de dispositivos conectados a Internet, y se espera que tanto esa cifra como el número de dispositivos vulnerables e infectados se

dupliquen en los próximos cinco años. Incluso si sólo la más pequeña fracción de estos dispositivos está infectada con botnets, los actores maliciosos tendrán un enorme potencial disruptivo a su disposición. Por tanto, es necesario un objetivo ambicioso de cero botnets.

Para lograr ese objetivo, los expertos en seguridad de la información deben primero hacer un mejor trabajo de medición de la actividad actual de las redes de bots y establecer objetivos graduales de reducción. A continuación, las naciones y las instituciones internacionales deberían trabajar para establecer el principio de que los Estados son responsables del daño que las redes de bots basadas en sus fronteras causan a otros. Cuando los gobiernos no pueden o no quieren ser responsables, puede estar justificado que otros estados tomen medidas, dentro o fuera del ciberespacio, para frustrar los efectos transfronterizos. Del mismo modo, en el ámbito de los proveedores de servicios de Internet (PSI), los buenos administradores de los espacios en línea deben responsabilizar a los demás PSI del mal tráfico que sale de sus redes. Hay que incentivar a los fabricantes de dispositivos vulnerables a convertirse en parte de redes de bots para que protejan sus dispositivos, y los revendedores de esos dispositivos deben utilizar su influencia para exigirles responsabilidades. Los proveedores de alojamiento, los registradores de nombres y otros componentes del ecosistema de Internet que son utilizados por las redes de bots deben ser presionados para que se vigilen a sí mismos y eviten que sus servicios sean utilizados con fines delictivos. Por último, cuando estas medidas no logren suprimir el crecimiento de las redes de bots, es necesario un esfuerzo internacional continuado para acabar con las redes de bots.

EL PODER DEL CERO

El cero es un concepto poderoso que se utiliza a menudo como herramienta para impulsar la acción política. Establecer un objetivo de cero para los resultados indeseables indica que cualquier suceso es inaceptable. A medida que se avanza, los sucesos se convierten en excepciones que desencadenan respuestas contundentes para entender lo que salió mal y evitar que se repitan los mismos patrones.

En el sector de la aviación, ningún pasajero de una aerolínea comercial registrada en Estados Unidos había muerto como resultado de un choque o accidente en más de nueve años hasta la reciente muerte de un pasajero del vuelo 1380 de Southwest en abril DE 2018. Ese incidente desencadenó una revisión exhaustiva de la seguridad de los motores y de los protocolos por los que se confirma la seguridad de los motores. Para el público volador, los reguladores, los accionistas de las aerolíneas y los operadores, cero es el único número aceptable de incidentes de seguridad.

Los responsables políticos están adoptando un enfoque similar en ámbitos como los accidentes de tráfico y la política de salud pública. Los alcaldes de Los Ángeles, Nueva York, Washington DC y otras treinta ciudades están llevando a cabo los llamados programas "Visión Cero" para las muertes de tráfico y de peatones. El esfuerzo se basa en un programa iniciado en Suecia hace veinte años. En el ámbito de la salud pública, se están llevando a cabo múltiples iniciativas de vacunación para conseguir cero infecciones en todo el mundo. Los esfuerzos de vacunación contra la viruela alcanzaron con éxito el objetivo de cero nuevas infecciones en 1978. Los esfuerzos para combatir la poliomielitis han dado lugar a solo veintidós nuevas infecciones en todo el mundo en 2017.

Por supuesto, eliminar por completo las redes de bots es probablemente un objetivo imposible. Del mismo modo, es poco probable que el mundo llegue a tener cero armas nucleares (el objetivo del movimiento Global Zero, adoptado por el presidente Barack Obama en

2009), al igual que no es probable que Suecia, Nueva York o Washington DC tengan cero muertes por accidentes de tráfico (el objetivo de Vision Zero). Pero a veces es necesario un objetivo extremo para centrar la política. Como muestran los datos, las tasas de infección extremadamente bajas (menos del 0,1%) en los Estados Unidos hoy en día) todavía puede permitir el montaje de potentes botnets. Por lo tanto, las tasas de infección tienen que estar muy por debajo de esa cifra para que sean efectivamente nulas.

MEDIR EL ESTADO ACTUAL *DE INFECCIONES DE BOTNETS*

Las infecciones de botnets varían enormemente en todo el mundo, con tasas de infección extremadamente bajas en los países no desarrollados, altas en los países en desarrollo y tasas de infección bajas y en aumento en el mundo desarrollado. En el mundo desarrollado, algunos países han tomado medidas activas para reducir las infecciones de botnets a casi cero. En particular, Finlandia tiene una asociación activa y voluntaria con sus proveedores de servicios de Internet para notificar a los propietarios de los sistemas infectados y, si es necesario, ponerlos en cuarentena. Finlandia tiene sistemáticamente una de las tasas de infección más bajas entre los países desarrollados. Otros esfuerzos nacionales han sido menos eficaces. Japón creó su Centro de Limpieza Cibernética en 2008 para reducir las tasas de infección pero, según la mayoría de las mediciones, sigue teniendo un importante problema de botnets. Alemania ha liderado un esfuerzo de varios años para reducir las infecciones de botnets nacionales, pero su enfoque no es ni de lejos tan eficaz como el de Finlandia. Estados Unidos, sin un enfoque nacional coordinado o un requisito legal, se compara favorablemente con muchos otros países que tienen tales enfoques o requisitos. Los datos proporcionados por Spamhaus, una organización internacional que rastrea las actividades de las redes de bots, sitúan a Estados Unidos en el número catorce de la lista de países con más infecciones de redes de bots (véase la tabla 1).

Tabla 1. PAÍSES CON MÁS INFECCIONES DE BOTNETS

Rank (most to least infected)	Country	Average number of bots
1	China	1,976,804
2	India	1,689,265
3	Brazil	606,216
4	Iran	566,353
5	Vietnam	560,720
6	Russia	506,982
7	Thailand	419,979
8	Turkey	412,390
9	Mexico	360,876
10	Indonesia	317,988
11	Pakistan	201,315
12	Philippines	166,177
13	Venezuela	156,718
14	United States	154,719
15	Egypt	148,298
16	Algeria	145,273
17	Japan	142,461
18	Italy	115,546
19	Argentina	113,470
20	Malaysia	101,093

Fuente: Spamhaus, 2018.

Sin embargo, en términos per cápita, las redes estadounidenses se encuentran entre las más limpias del mundo. Entre los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), Estados Unidos tiene la octava red más limpia (véase la tabla 2), posiblemente debido a las menores tasas de software pirata o no soportado y a la prevalencia del software antivirus. Alemania ocupa el duodécimo lugar de la lista y Japón el decimosexto. [4]

Sin embargo, a la luz de los daños pasados y potenciales que causan las redes de bots, incluso las tasas de infección que están muy por debajo de la décima parte del 1% son demasiado altas, dado el gran y creciente número de sistemas en Internet. Aunque Estados Unidos tiene una tasa de infección que se encuentra entre las más bajas del mundo, el país también fue uno de los cinco principales países de origen de los ataques DDoS en cada trimestre de 2017 (véase la tabla 3). [5] Por lo tanto, la gestión del problema de las redes de bots requiere llevar el número absoluto de infecciones a cero o casi.

Tabla 2. CLASIFICACIÓN DE LAS TASAS DE INFECCIÓN DE BOTNETS ENTRE LOS PAÍSES DE LA OCDE

Rank (least to most infected)	Country	% of IP addresses infected
1	Denmark	0.0258%
1	Finland	0.0258%
2	Switzerland	0.0353%
3	Netherlands	0.0549%
4	France	0.0574%
5	United Kingdom	0.0583%
6	Canada	0.0608%
7	Belgium	0.0627%
8	United States	0.0629%
9	Estonia	0.0816%
10	New Zealand	0.0830%
11	Sweden	0.0835%
12	Germany	0.1039%
13	Austria	0.1079%
14	Korea	0.1123%
15	Iceland	0.1171%
16	Japan	0.1204%
17	Luxembourg	0.1430%
18	Slovakia	0.1447%
19	Czech Republic	0.1509%

Fuente: Spamhaus, 2018.

Tabla 3. PRINCIPALES PAÍSES DE ORIGEN DE LOS ATAQUES DE DDoS, 2017

Q4 2017		Q3 2017		Q2 2017		Q1 2017	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
Germany	30% 128,350	Germany	22% 58,746	Egypt	32% 44,198	United States	44% 594,986
China	28% 118,716	United States	14% 38,628	United States	8% 11,113	United Kingdom	13% 177,579
United States	8% 36,441	India	7% 19,722	Turkey	5% 7,049	Germany	7% 87,780
Ecuador	3% 14,685	China	6% 15,323	China	4% 5,711	Canada	5% 60,581
Austria	3% 13,503	Mexico	5% 13,501	India	4% 5,224	Brazil	3% 43,863

Fuente: McKeay, "Estado de Internet / Seguridad: Informe del cuarto trimestre de 2017".

POR QUÉ PERSISTEN LAS REDES DE BOTS

A pesar de los esfuerzos realizados para hacer frente a las redes de bots, el número de redes de bots y de sistemas infectados sigue creciendo. Los esfuerzos anteriores han sido desarticulados y se han centrado por separado en las notificaciones de los ISP a los propietarios de los sistemas infectados o en los esfuerzos coordinados de las fuerzas del orden para detener a los llamados botmasters y desbaratar la infraestructura que utilizan para controlar sus redes de bots.

La Comisión Federal de Comunicaciones (FCC) colaboró con los principales ISP en el marco del Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones (CSRIC) para elaborar el Código de Conducta Anti-Bot en 2012.[6] Este código es un esfuerzo voluntario para educar a los clientes sobre las botnets, detectar las actividades de las botnets, notificar a los clientes de las sospechas de infección y proporcionar información sobre cómo remediar las infecciones de las botnets. Aunque muchos ISP adoptaron las prácticas promovidas en el código de conducta, su eficacia sigue siendo incierta.

En abril DE 2013, el FBI anunció la Operación Clean Slate, cuyo objetivo declarado era reducir o eliminar las redes de bots que amenazaban la seguridad económica de Estados Unidos y la privacidad de sus ciudadanos.[7] Aunque el FBI tuvo una serie de éxitos en el cierre de algunas redes de bots, estos esfuerzos no se han traducido en una reducción medible del número de redes de bots, el número de dispositivos infectados o el daño que causan las redes de bots.

Es necesario un enfoque más amplio que vaya más allá de la aplicación de la ley y la notificación y cuarentena de los ISP para abordar el problema desde múltiples vectores. Los retos de la eliminación de las redes de bots provienen de tres categorías: las tecnologías existentes y las nuevas; las cuestiones operativas, organizativas y de procesos; y la política y la economía.

La facilidad de la suplantación. Los delincuentes que dirigen los ataques DDoS aprovechan cualquier oportunidad para cubrir sus huellas y dificultar la identificación del origen del ataque por parte de los responsables. Dado que los ataques DDoS no requieren una comunicación bidireccional, sino que simplemente inundan a la víctima con tráfico, los responsables de los bots suelen programar sus programas maliciosos para "falsificar" la dirección del protocolo de Internet (IP) de la que proceden los paquetes de datos, es decir, para que parezca que los datos proceden de una dirección diferente, de modo que sea difícil identificar las fuentes del ataque. Estados Unidos tiene el mayor número de bloques de IP falsificables, pero éstos representan sólo el 4,8% de todas sus direcciones IP en los datos de la muestra. En muchos países en desarrollo, el 100% de los bloques de IP son falsificables. [8] A finales de la década de 1990, los miembros de la comunidad de seguridad de Internet desarrollaron un protocolo para abordar este problema, llamado Best Common Practice 38. El protocolo pedía a los proveedores de servicios de Internet (ISP) que se comprometieran a proteger la privacidad de los usuarios. El protocolo pedía a los ISP que aplicaran un "filtrado de salida", en el que se bloquearan todos los paquetes que afirmaran proceder de direcciones IP que no tuvieran asignadas.

Alojamiento a prueba de *balas. Los proveedores* de alojamiento a prueba de balas son aquellos que albergan actividades delictivas que las empresas de alojamiento legítimas no acatan. Ningún sistema mejorado de denuncia de abusos cambiará la forma de operar de los proveedores de alojamiento a prueba de balas. Suelen estar ubicados en países con una débil aplicación de la ley, altos niveles de corrupción o malas relaciones con Occidente. Estos proveedores, que a menudo ofrecen servicios a bajo coste, afirman que no tienen los recursos necesarios para vigilar los contenidos de los usuarios o responder a todas las denuncias de abusos. Dado que casi siempre albergan algunos negocios legítimos que se ven atraídos por los servicios de bajo coste, cerrarlos de golpe o detener todo el tráfico procedente de ellos no es una respuesta adecuada.

El crecimiento del IoT. Las tecnologías IoT dificultan la gestión del problema de las redes de bots. El gran número de dispositivos significa que incluso una baja tasa de infección puede dar a los actores maliciosos acceso a un número increíblemente grande de dispositivos comprometidos. Además, el hecho de que estos dispositivos se configuren y se olviden significa que es menos probable que los propietarios instalen

actualizaciones de software o protejan sus dispositivos. Gran parte del crecimiento previsto de los dispositivos IoT se debe a su bajo coste, lo que conduce a prácticas de desarrollo deficientes y, por tanto, a dispositivos menos seguros. Además, el 60% de las aplicaciones de Internet contienen componentes de código abierto con vulnerabilidades de software conocidas. [9]

La aparición de las criptomonedas. Gran parte del valor que los delincuentes obtienen al operar redes de bots y esquemas de extorsión DDoS proviene de criptomonedas como bitcoin y ethereum. Los delincuentes inician un ataque DDoS y luego exigen un pago en criptomoneda para detenerlo, normalmente mucho menos de lo que cobraría una empresa de mitigación de DDoS. Las criptomonedas permiten a los delincuentes exigir pagos de rescate que no son fáciles de rastrear a través del sistema financiero: se acabaron los días de los maletines sin marca de billetes de 100 dólares no consecutivos. Aunque todas las transacciones de bitcoin se registran públicamente en la cadena de bloques asociada, los individuos asociados a estas transacciones son desconocidos por diseño. El desarrollo de los servicios de "volteo" que combinan las transacciones de criptodivisas no delictivas con las delictivas dificulta que las fuerzas de seguridad se centren en los puntos vulnerables que quedan en el sistema, como cuando los delincuentes tratan de convertir las monedas virtuales en monedas fiduciarias. Las monedas más recientes, como Monero, Zcash y Dash, parecen estar diseñadas expresamente para realizar transacciones delictivas. [10]

CUESTIONES OPERATIVAS, ORGANIZATIVAS Y DE PROCESOS

La complejidad de los desmantelamientos de redes de bots. El desmantelamiento coordinado de las redes de bots por parte de las fuerzas del orden, los proveedores de servicios de Internet, las empresas de software, las empresas de seguridad y el mundo académico puede reducir drásticamente el número de máquinas infectadas en todo el mundo y los males asociados. Sin embargo, se ha demostrado que es difícil mantener los esfuerzos persistentes a lo largo del tiempo. Los desmantelamientos de botnets no son un trabajo a tiempo completo. En un periodo de diez años, se produjeron veintitrés desmantelamientos parciales o totales de botnets (véase la tabla 4). Los desmantelamientos se producen a trompicones: EN 2012 se produjeron cuatro desmantelamientos de botnets, seguidos de tres en 2013, uno en 2014, tres en 2015, uno en 2016 y dos en 2017.[11] En los desmantelamientos más eficaces interviene un amplio abanico de partes que actúan de forma concertada para atacar la red de bots desde múltiples ángulos: se utilizan órdenes judiciales para confiscar servidores y dominios web en todo el mundo, las fuerzas de seguridad detienen a miembros conocidos y accesibles de la organización delictiva que está detrás de la red de bots, los proveedores de servicios de Internet bloquean el tráfico, los proveedores de software introducen parches y, bajo la autoridad de las fuerzas de seguridad, los expertos técnicos intentan hacerse con el control o eliminar el malware subyacente a la vez.

El liderazgo de estos esfuerzos ha sido difuso. Ninguna organización es responsable de coordinar los retiros. Sólo Microsoft ha perseguido a más de una docena. Empresas de ciberseguridad como Crowd Strike, FireEye, Lastline, Symantec y TrendMicro han liderado otros esfuerzos. El FBI, el Departamento de Justicia de Estados Unidos y el Servicio Secreto también han coordinado sus esfuerzos.

Tabla 4. PRINCIPALES DESMANTELAMIENTOS DE BOTNETS EN LA ÚLTIMA DÉCADA

Date	Botnet
November 2008	McColo
November 2009	Mega D
December 2009	Mariposa
February 2010	Waledac
September 2010	Pushdo
November 2010	DNSCHanger
March 2011	Rustock
April 2011	Coreflood
November 2011	Rove Digital
March 2012	Zeus Botnet
July 2012	Grum
September 2012	Nitol
December 2012	Butterfly Bot
February 2013	Bamital
June 2013	Citadel
December 2013	Sirefef/ZeroAccess
June 2014	Gameover Zeus
February 2015	Ramnit
April 2015	Simda
December 2015	Dorkbot
December 2016	Avalanche
April 2017	Kelihos Botnet
December 2017	Gamarue/Andromeda

Fuente: Investigación de los autores.

Organizaciones como el Centro Europeo de Ciberdelincuencia de Europol, el Consorcio de Sistemas de Internet, el Grupo de Trabajo contra el Malware, el Grupo de Trabajo Mariposa, la Alianza Nacional de Formación Ciberforense y Spamhaus han coordinado los desmantelamientos. Estos esfuerzos se basan en una reserva limitada de talento técnico y ponen a prueba los recursos de las organizaciones que contribuyen al esfuerzo. En resumen, el desmantelamiento de redes de bots no es el trabajo diario de nadie.

Procesos rotos para la notificación de abusos. Los procesos para denunciar ataques DDoS, otras actividades maliciosas y sistemas vulnerables no funcionan. Los proveedores de alojamiento y los ISP suelen ignorar las denuncias de abuso o las abordan con lentitud. La denuncia efectiva de los abusos depende a menudo de una red informal -y no siempre eficaz- de personas en empresas de todo el mundo. Los esfuerzos de una víctima de Mirai ilustran bien este problema: A medida que el ataque contra ProxyPipe, un proveedor de mitigación de DDoS para servidores de Minecraft, continuaba, Robert Coelho, vicepresidente de la compañía, no pudo mantener accesibles los servidores de sus clientes. Recurrió a la presentación de quejas por abuso a los proveedores de alojamiento y a los ISP que apoyaban al servidor de mando y control del botmaster que dirigía el ataque. Coelho llegó a la conclusión de que el servidor de control se gestionaba desde un conocido proveedor de alojamiento a prueba de balas en Ucrania. Ese proveedor, BlazingFast, no respondió a los informes de abuso de Coelho, ni tampoco el servicio de mitigación de DDoS de BlazingFast, Voxility. Coelho se dirigió entonces a cuatro proveedores de servicios de Internet, que no prestaron asistencia, antes de que un quinto proveedor, la finlandesa TeliaSonera, respondiera a su petición y cortara la conectividad del servidor de control a través de su red. "La acción de Telia redujo el tamaño de los ataques lanzados por la botnet a 80 Gbps", un nivel de tráfico que ProxyPipe podía gestionar. [12]

Sin embargo, un sistema más rápido y automatizado para denunciar los abusos podría crear sus propios problemas. Incluso para las empresas que pretenden ser buenas administradoras del ciberespacio, un sistema de este tipo podría dar lugar al equivalente del "swat- ting" en línea, donde los sistemas de abuso se utilizan indebidamente para cerrar la actividad legítima. [13] Algunas empresas han desarrollado redes verificadas entre partes de confianza para automatizar este proceso. Los proveedores de alojamiento y los ISP que no responden se enfrentan a pocas repercusiones. Al carecer de recursos de terceros, las víctimas de actividades maliciosas tienen que trabajar por su cuenta con empresas a menudo indiferentes y hostiles.

Escasos mecanismos de cooperación internacional. El papel de los equipos nacionales de respuesta a emergencias informáticas (CERT) está mal definido dentro del ecosistema de Internet: sólo algunos tienen capacidad para prestar asistencia a gobiernos y empresas extranjeras. En los países con proveedores nacionales de telecomunicaciones y leyes que favorecen la notificación y la cuarentena, los CERT nacionales desempeñan un papel útil. En Estados Unidos, el Computer Emergency Readiness Team sólo tiene una capacidad limitada de asistencia en caso de ataque DDoS.

La dificultad de identificar a los propietarios de los sistemas infectados.

En las redes en las que se encuentran, a menudo sólo pueden llegar hasta el ISP que les proporciona el servicio. En Estados Unidos, los proveedores de servicios de Internet no están autorizados a compartir información sobre sus clientes con terceros, en virtud de la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA). Esta prohibición se extiende a las agencias gubernamentales, a menos que se emita una citación de las fuerzas del orden. A nivel internacional, la identificación de los propietarios de sistemas también se ve obstaculizada por leyes locales como el Reglamento Global de Protección de Datos (GDPR) de la Unión Europea. Ahora que está entrando en vigor, el GDPR considera las direcciones IP como datos personales sujetos a protección. Por lo tanto, los esfuerzos para notificar al propietario del sistema y alentar la acción de remediación tienen que depender del ISP (a menos que el sistema esté en la red de una gran corporación con su propio espacio de direcciones). Muchos ISP han sido reacios a notificar activamente a los clientes de las infecciones debido a los costes y a la preocupación por la privacidad.

CUESTIONES POLÍTICAS Y ECONÓMICAS

Incentivos económicos que favorecen al atacante. Según el experto en ciberseguridad Jim Lewis, "una red de bots que cuesta sólo 60 dólares al día puede infligir hasta 720.000 dólares en daños a las organizaciones víctimas, y los hackers que controlan las redes de bots disfrutan de un margen de beneficio de más del 70% al alquilar sus servicios a otros delincuentes. " [14] Deben identificarse y aplicarse intervenciones que aumenten los costes de llevar a cabo estos ataques, además de reducir los beneficios.

Incentivos perversos para la mitigación de DDoS. Las empresas que ofrecen servicios de mitigación de DDoS no quieren que los ataques cesen, sino que continúen a niveles manejables. Como dijo Coelho, vicepresidente de ProxyPipe, en un intercambio de textos con el botmaster que está detrás de Mirai, "sólo queríamos que los ataques fueran más pequeños"; no dijo que quisiera que los ataques se detuvieran. [15]

La mitigación de DDoS es un negocio en crecimiento. Empresas como Akamai y Cloudflare ofrecen servicios de tarifa plana que actúan como una póliza de seguro y alinean adecuadamente los incentivos para que los proveedores de mitigación tengan interés en limpiar el ecosistema. Los bucles de retroalimentación entre las víctimas de DDoS y las fuentes de las redes de bots podrían acabar reduciendo el número de bots a cero, pero todavía es un trabajo en curso.

Costes indirectos de las botnets. *Las* botnets no suelen causar daños a los sistemas que infectan, sino a terceros.

El ancho de banda no parece ser una preocupación significativa para los propietarios y operadores de la mayoría de los sistemas infectados. Algunos individuos no se preocupan por el robo de su información personal y apenas notan el impacto en el rendimiento de sus ordenadores mientras minan criptomonedas para otros. Algunas empresas hacen la vista gorda ante el robo de su propiedad intelectual. Sin embargo, aunque los responsables de los bots extraen todo el valor que pueden de los sistemas infectados, el verdadero valor de mantener una red de bots es utilizarla para atacar a terceros.

La *preocupación por la privacidad y la falta de incentivos económicos para la actuación de los ISP*. La neutralidad de la red ha contribuido en el pasado al enfoque de no intervención de los ISP, que sostienen que, como transportistas comunes, están obligados a transmitir el tráfico a menos que cause un daño directo a sus propios sistemas, y no a otros ISP o a los usuarios finales que se encuentran más abajo. Con la terminación de las normas de neutralidad de la red por parte de la FCC, la preocupación de los ISP por violar la neutralidad de la red al bloquear la actividad de las redes de bots ha sido resuelta. Además, los cambios introducidos en la ECPA por la Ley de Ciberseguridad de 2015 otorgan a los ISP amplias exenciones de responsabilidad por bloquear el tráfico malicioso. El problema más amplio sigue siendo que muchos ISP no ven la lucha contra las botnets como parte de su modelo de negocio; filtrar el tráfico DDoS para los clientes o proporcionar ancho de banda adicional a las víctimas es un buen negocio. No es probable que los ISP se decidan a bloquear el acceso de sus clientes a Internet, al menos en el mercado estadounidense. Un enfoque más prometedor, que AT& T y CenturyLink están probando, no trata de limpiar las infecciones, sino que interrumpe su mandato y control en la red para que el botmaster no pueda dirigir las actividades de los bots, haciendo que la amenaza que suponen sea inerte.

RECOMENDACIONES

En la Orden Ejecutiva 13800, el Presidente de los Estados Unidos, Donald J. Trump, ordenó al Departamento de Comercio y al Departamento de Seguridad Nacional que trabajaran con el sector privado para identificar formas de "reducir drásticamente las amenazas perpetradas por ataques automatizados y distribuidos (por ejemplo, botnets)". "El informe resultante, "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats", publicado en mayo DE 2018, es un recurso invaluable para definir el problema, y muchas de sus recomendaciones informan las que se presentan a continuación. [16] Lo que falta en este esfuerzo que fue informado por docenas de organizaciones con un interés en la reducción de la amenaza de los botnets es un objetivo claro y medible. Establecer un objetivo global de cero botnets es el primer paso para abordar el problema.

A partir de ahí, deben buscarse compromisos nacionales para lograr cero botnets en las redes nacionales. Los objetivos provisionales y los sistemas para medir el progreso hacia esos objetivos son cruciales. Estos objetivos podrían abordarse principalmente dentro de los límites nacionales. Los objetivos deberían establecerse en plazos específicos basados en el número de dispositivos conectados en un país. Los países desarrollados deberían tener requisitos más estrictos y plazos más rápidos, con requisitos iniciales menos onerosos para los países en desarrollo.

ESTABLECER UN OBJETIVO GLOBAL Y MEDIR A LOS ESTADOS EN FUNCIÓN DE ÉL

Para lograr la eliminación de las redes de bots, es necesario establecer objetivos intermedios y medir los avances en relación con ellos. Los objetivos de las botnets deben ser acordados por los líderes políticos, junto con la sociedad civil y los ejecutivos de las empresas globales. Establecer estos objetivos y hacer que los principales socios los acepten es el primer paso más importante para crear un movimiento.

Estos objetivos deberían comenzar con un acuerdo para lograr que los principales proveedores de servicios de Internet (ISP) tengan cero botnets, lo que podría ser tan sencillo como un apretón de manos en el podio entre los presidentes de Estados Unidos y China. A continuación, una comunidad más amplia puede desarrollar métricas, normas e implementación más concretas. Los implicados pueden corregir el rumbo a medida que ven los éxitos y los fracasos en el cumplimiento de estos hitos, y recoger las lecciones aprendidas de los países y las empresas que tienen éxito. Llegar a un acuerdo sobre los parámetros y medir el éxito en función de ellos será difícil. Spamhaus y otras organizaciones llevan años haciendo un seguimiento de las redes de bots y las tasas de infección por países. [17] Asimismo, la Cyber Green Initiative ha estado trabajando para hacer un seguimiento científico de las redes de bots. [18] Estos grupos pueden medir el progreso hacia las redes de bots cero.

ESTABLECER EL PRINCIPIO DE RESPONSABILIDAD DEL ESTADO POR LOS DAÑOS CAUSADOS POR LOS BOTNETS

A medida que los retos del siglo XXI, como el terrorismo, la proliferación nuclear y la contaminación, se han convertido en retos de seguridad nacional, las nociones de soberanía nacional también han cambiado. En lugar de ser un derecho absoluto de los Estados, la soberanía viene ahora acompañada de una responsabilidad soberana hacia los ciudadanos de los Estados y de obligaciones soberanas hacia otros Estados. [19] Las redes de bots causan daños a los individuos, a las empresas y a los Estados, pero sólo cuando el daño es de naturaleza transfronteriza se convierte en un problema de política internacional, en el que el Estado que causa el daño tiene una obligación soberana con otros Estados para abordarlo. [20] Según esta línea de razonamiento, los Estados podrían optar por permitir altos índices de infecciones de botnets siempre que el daño que causen se limite a su propio territorio. Sin embargo, deberían ser considerados responsables por el sistema internacional por los daños causados a otros Estados si no trabajan de forma proactiva y cooperativa para responder a ellos.

FOMENTAR LA COOPERACIÓN Y LA ACCIÓN INTERNACIONAL

Los Estados deberían tener incentivos tanto de zanahoria como de palo para tomar medidas para reducir la prevalencia de botnets en sus redes nacionales. Puede ser útil situar a los Estados en un espectro de responsabilidad. En primer lugar, los Estados que utilizan activamente las redes de bots para coaccionar a otros Estados: éstos deberían ser el objetivo específico de las instituciones internacionales. A continuación estarían los Estados que albergan a las empresas criminales que están detrás de las operaciones de las redes de bots. Los Estados que simplemente son incapaces de vigilar lo que ocurre dentro de sus fronteras estarían en la parte inferior del espectro.

Con este marco en mente, se podrían utilizar incentivos para ayudar a los que se encuentran en el extremo inferior del espectro a lograr reducciones. Los Estados que utilizan activamente las redes de bots o que las albergan podrían ser objeto de sanciones, como por ejemplo, la vergüenza, la limitación de la inversión y las sanciones. Los países desarrollados tendrán que ayudar a los países en desarrollo a reducir la actividad de las redes de bots, entre otras cosas, ayudando a resolver problemas de larga data en el ecosistema, como la prevalencia del software pirata. El gobierno de Estados Unidos, las naciones afines y las empresas interesadas en reducir la actividad de las redes de bots deberían financiar un informe anual elaborado por una organización independiente para hacer un seguimiento de los éxitos conseguidos a nivel estatal en la reducción de las redes de bots.

Una vez establecidas las obligaciones internacionales, la falta de respuesta podría proporcionar motivos razonables para que las naciones tomen medidas limitadas para prever, de la manera más estrecha posible, el daño sin causar más daño a cambio. Por ejemplo, en el caso de que un país no establezca mecanismos para recibir y actuar sobre las denuncias de abuso de manera oportuna, un gobierno extranjero podría autorizar el desmantelamiento de un servidor de mando y control. Tomar medidas como ésta debe hacerse como último recurso, ya que los Estados podrían percibirlas como una violación de la soberanía y una acción hostil, por muy limitada que sea.

CREAR INCENTIVOS PARA QUE LAS ISP LIMPIEN SUS REDES

Algunos ISP detectan cuando un cliente está infectado con malware, se lo

notifican a esa persona por mensaje de texto y la desvían a un "jardín amurallado" en el que no puede acceder a Internet en general hasta que se limpie el ordenador, a veces con ayuda del ISP. Lo más importante es que no se excluye a la persona de Internet, ya que eso limitaría la libertad de expresión, sino que el l dispositivo que está causando daños a otros. Sin embargo, aunque esta práctica lleva más de una década en vigor, no se acepta como una responsabilidad común de los ISP.

Aunque los ISP desconfían de la regulación en este ámbito, los ISP, como comunidad, podrían autocontrolarse. Los ISP podrían acordar una norma según la cual, por ejemplo, un ISP con cien millones de dispositivos o un petabyte de tráfico al mes podría tener permitido un determinado porcentaje de dispositivos infectados, o de emisiones. Si el ISP tuviera más que eso, tendría que pagar una cuota o comprar créditos de una red más limpia hasta que pudiera reducir el número por debajo del umbral.

ESTABLECER NORMAS PARA EVITAR QUE LOS DISPOSITIVOS SE VEAN FÁCILMENTE COMPROMETIDOS

Como concluye el informe al presidente, "se necesitan líneas de base de capacidades de seguridad basadas en el rendimiento -que identifiquen conjuntos de normas, especificaciones y mecanismos de seguridad voluntarios que representen la combinación de las mejores prácticas para la seguridad del ciclo de vida para un entorno de amenaza concreto- para acelerar el desarrollo y el despliegue de dispositivos y sistemas del IoT que sean menos vulnerables a las amenazas a lo largo de su ciclo de vida."[21] Lo que no hace el informe es identificar quién debe desarrollar estas normas; sin embargo, el Instituto Nacional de Normas y Tecnología (NIST) ya ha completado gran parte del trabajo preliminar para producir dichas normas y tiene un excelente historial de trabajo con la industria. El presidente o el secretario de comercio deberían ordenar al NIST que establezca rápidamente normas para la seguridad de los dispositivos IoT. Estas normas deberían incluir lo siguiente.

- *Eliminar las vulnerabilidades conocidas en el momento de la producción. Los* componentes de código abierto deben ser las versiones más actualizadas, y los fabricantes de dispositivos deben analizar las vulnerabilidades del código que escriben.

- *Seguir las mejores prácticas para el endurecimiento de los dispositivos.* Las normas también deben exigir a los fabricantes que pongan en marcha medidas que dificulten a los adversarios poner en peligro los dispositivos.

- *Hacer que los dispositivos sean actualizables.* Es probable que la nueva tecnología operativa permanezca en el entorno mucho más tiempo que la tecnología de oficina, por lo que es crucial que los dispositivos de IoT tengan la capacidad de realizar actualizaciones remotas y automáticas para solucionar los fallos de seguridad. Dichas actualizaciones deben ser automáticas por defecto, y los usuarios deben poder optar por probar las actualizaciones antes de desplegarlas.

- *Mantener una "lista de materiales" para los componentes de software.* A medida que se descubren vulnerabilidades en los componentes de código abierto, los propietarios de la tecnología deben saber si el software se ha construido con componentes seguros.

- *Proporcionar contraseñas únicas para cada dispositivo.* Toda la producción de dispositivos IoT suele utilizar las mismas contraseñas por defecto. Cambiar este procedimiento eliminaría el método más fácil que utilizan los atacantes para hacerse con el control de los dispositivos. [22]

UTILIZAR LA PRESIÓN DEL MERCADO PARA INCENTIVAR A LOS FABRICANTES DE DISPOSITIVOS A CUMPLIR LAS NORMAS

Al igual que no se pueden vender coches que contaminen en exceso, los distribuidores deben negarse a vender productos cuya seguridad no haya sido demostrada. *Consumer Reports* y otras organizaciones están desarrollando calificaciones de ciberseguridad para los dispositivos electrónicos. [23] Este esfuerzo tardará en madurar, pero es el mecanismo adecuado para reducir la difusión de dispositivos inseguros. Si se hace bien, puede alinear mejor los mercados y los incentivos a bajo coste pero con gran efecto.

Más allá de la transparencia, los minoristas deberían negarse a vender productos que no cumplan las normas del NIST. Walmart y Amazon ya son los "reguladores" más poderosos en una serie de cuestiones: especifican el tamaño de los envases y la forma del embalaje que permiten. Exigir que los dispositivos IoT cumplan las normas de seguridad haría más que casi cualquier otra acción para reducir la prevalencia de las redes de bots. La decisión de BestBuy de dejar de vender el software antivirus de Kaspersky Lab tras
Las afirmaciones del gobierno estadounidense de que estaba vinculado al espionaje del Kremlin es un prece- dente para tal acción.

Acciones similares sobre los dispositivos inseguros podrían tener un efecto significativo. Los bancos, a menudo víctimas de ataques DDoS, deberían presionar a los fabricantes y revendedores de dispositivos negándose a conceder préstamos a las empresas que no cumplan las normas. Los reguladores de las infraestructuras críticas deberían prohibir los dispositivos que no cumplan la norma. Aunque en el clima político actual es poco probable que se concedan nuevos poderes reguladores, los reguladores con autoridad existente deberían establecer este requisito.

LLAMAR A LOS FACILITADORES DE LA ACTIVIDAD DE LAS REDES DE BOTS

Las campañas exitosas que emplean el concepto de cero (por ejemplo, en accidentes de tráfico o accidentes aéreos) miden activamente los avances y dan a conocer tanto los éxitos como los fracasos en el intento de alcanzar ese objetivo. Esta trans- parencia podría ayudar a presionar a los responsables de la actividad de las redes de bots.

Los ciberdelincuentes suelen recurrir a los principales servicios de computación en la nube cuando necesitan recursos informáticos para el mando y control de los ataques DDoS. En 2017, OVH, el objetivo de los ataques DDoS llevados a cabo por Mirai, albergó el mayor número de servidores de mando y control de botnets del mundo; Amazon fue el segundo. [24 LA] mayoría de estos servidores de mando y control se crearon simplemente comprando los servicios de la empresa, normalmente con números de tarjeta de crédito robados comprados en la web oscura. El registrador estadounidense NameCheap es el lugar más popular para que los operadores de botnets compren direcciones web para el mando y control (los botnets necesitan contactar con los dominios web para recibir instrucciones). NameCheap representó 11.878 registros para el funcionamiento de botnets en 2017, una cuarta parte de todos los registros de este tipo.

Las fuerzas del orden, los accionistas y los clientes podrían presionar a los vendedores de computación en la nube y de dominios web favorecidos por los ciberdelincuentes para que dificulten mucho más el funcionamiento de las redes de bots. Identificar y eliminar rápidamente las cuentas implicadas en esta actividad delictiva está dentro de la capacidad técnica de estas empresas, pero, si no se les presiona para que lo hagan, no les interesa económicamente. Estados Unidos y sus aliados también deberían presionar a los países en los que germina esta actividad mediante la denuncia, las sanciones y el enjuiciamiento penal de los botmas y los servicios que permiten su funcionamiento.

Si los proveedores de servicios legítimos se vigilan a sí mismos y obligan así a los grupos delictivos a utilizar proveedores que hacen la vista gorda a sabiendas, será posible aislar y castigar a estos grupos. En el pasado, los proveedores de servicios de Internet han bloqueado el acceso de dichos proveedores a grandes partes de Internet. Sin embargo, la adopción de estas medidas de forma más amplia sólo será posible una vez que estos grupos se distingan más del alto nivel actual de actividad maliciosa. Los ISP ya están experimentando con formas mecanizadas de eliminar el tráfico malicioso.

ESTABLECER UNA ORGANIZACIÓN INDEPENDIENTE PARA EL DESMANTELAMIENTO DE BOTNETS

Incluso cuando los derribos ofrecen resultados increíbles, el éxito suele ser el resultado de un nivel de trabajo excepcional. Esto debería cambiar para que los desmantelamientos se produzcan a escala, y que los beneficios superen a los ingresos. Como explicaba un editor en un blog de TechTarget, "si determinamos que una red de bots está enviando millones de mensajes al día -los servidores de mando están en Rusia, parte de la infraestructura está en España, y los bots están en Norteamérica, tiene que haber una forma de que todos estos grupos cooperen en tiempo real, o muy rápidamente. Porque cuando se desmantela una red de bots, si no se desmantela toda la estructura al mismo tiempo, es muy fácil que estos tipos tomen el control y redirijan todo ese tráfico a otro lugar"

Los desmantelamientos de redes de bots implican un trabajo técnico muy cualificado y que requiere mucho tiempo, y no son un trabajo a tiempo completo para nadie. Pero debería serlo. Una posibilidad sería establecer organizaciones de colaboración para incidentes cibernéticos (CICO). [26] Uno de estos grupos podría centrarse en cada tipo de incidente importante, como la lucha contra los DDoS o los brotes de malware. El CICO de lucha contra las redes de bots sería "global y estaría dirigido por el sector privado, con miembros que incluyeran las organizaciones globales que han desempeñado el mayor papel en los desmantelamientos, como, por ejemplo, Microsoft, FireEye y el Departamento de Justicia". "Este grupo trabajaría con CICOs relacionados contra el software malicioso y los ataques DDoS, ya que a menudo están relacionados. Estos grupos "no pueden ser simplemente una nueva organización con gastos adicionales. Más bien, el objetivo de un CICO debería ser agilizar el proceso de respuesta actual para un tipo de incidente; proporcionar un paraguas para facilitar ese trabajo o ampliarlo".[27]

Una organización relativamente pequeña, financiada con 10 millones de dólares al año durante un periodo de cinco años, probablemente sería capaz de llevar a cabo múltiples desmantelamientos al año. Esta organización también podría medir las redes de bots a nivel mundial y proporcionar asistencia técnica a los países y empresas que luchan por reducir sus tasas de infección. La financiación de una organización de este tipo podría ser un reto, pero teniendo en cuenta los costes que causan los ataques DDoS, el apoyo a una organización que reduzca la amenaza sería de interés para el sector financiero, el sector de las telecomunicaciones, los proveedores de computación en la nube y las agencias gubernamentales.

Estos grupos deberían ser internacionales desde su nacimiento, y no un crecimiento de las burocracias nacionales de ciberseguridad. Los CERT nacionales deberían participar, pero la agilidad y la facilidad de coordinación transfronteriza necesarias probablemente sean demasiado difíciles para los gobiernos.

CONCLUSIÓN

La amenaza de las redes de bots para la salud de Internet y la economía digital moderna que depende de ella sigue creciendo. Con los miles de millones de nuevos dispositivos que se incorporarán a Internet en la próxima década, ha llegado el momento de establecer un régimen internacional que trabaje para mantener los dispositivos vulnerables fuera de Internet, mitigar los dispositivos una vez infectados y responder a los problemas que causan los dispositivos infectados. En ausencia de esfuerzos sostenidos y organizados para combatir este problema, las redes de bots y los actores maliciosos que las controlan se llevarán una parte cada vez mayor del valor creado por Internet y los sistemas conectados a ella.

Cero botnets es un grito de guerra eficaz para motivar a la dispar coalición de fabricantes de tecnología, proveedores de servicios de Internet, consumidores, empresas de ciberseguridad, organizaciones sin ánimo de lucro y organismos policiales que son necesarios para reducir las infecciones de botnets a niveles en los que no supongan una amenaza para el funcionamiento continuado de Internet o de las organizaciones que operan en ella. Si se motiva adecuadamente, una coalición de este tipo podría, con el tiempo, reducir las tasas de infección de las redes de bots, aumentar los costes de los actores maliciosos para operarlas y negarles el valor por hacerlo.

NOTAS FINALES

1. Joy Ma y Tim Matthews, "The Underground Bot Economy: How Bots Impact the Global Economy", Imperva Incapsula, 5 de julio de 2016, http://incapsula.com/blog/how -bots-impactan-economía-global.html.

2. "Project Shield", Google, consultado el 21 de mayo de 2018, http://projectshield.withgoogle .com/public.

3. James Lewis, "Economic Impact of Cybercrime-No Slower Down", Center for Strategic and International Studies y McAfee, febrero de 2018, http://mcafee.com /empresa/en-us/activos/informes/restringidos/impacto-económico-ciberdelito.pdf.

4. Datos para las tablas 1 y 2 proporcionados por Spamhaus para 2018; análisis de datos completado por Justin Haner, Northeastern University.

5. Martin McKeay, ed., "Estado de Internet / Seguridad: Informe del cuarto trimestre de 2017", Akamai, http://akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state -de-la-internet-seguridad-informe.pdf.

6. *Informe final: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)*, Communications Security, Reliability and Interoperability Council (Federal Communications Commission: Washington, DC, 2012), http://m3aawg.org/system /files/20120322-wg7-final-report-for-csric-iii_5.pdf.

7. *Acabar con las redes de bots*, 113th Cong. (2014) (declaración de Joseph Demarest, Director Adjunto de la División Cibernética, FBI), http://fbi.gov/news/testimony/taking-down -botnets.

8. Spoofer, "Country Stats for Last Year of Data", Center for Applied Internet Data Analysis, modificado por última vez el 8 de junio de 2018, http://spoofer.caida.org/country_stats.php.

9. Black Duck Software, "2017 Open Source Security and Risk Analysis", http:// blackducksoftware.com/sites/default/files/images/Downloads/Reports/ USA /OSSRA17_Rpt_UL.pdf.

10. Kieran Corcoran, "Law Enforcement Has a Massive Problem With These 3 Cryptocurrencies", *Business Insider*, 27 de febrero de 2018, http://businessinsider.com/problemas de aplicación de la ley-con-monero-zcash-cryptocurrencies-2018-2.

11. Investigación de los autores.

12. Brian Krebs, "¿Quién es Anna-Senpai, la autora del gusano Mirai?", *Krebs on Security* (blog), 17 de enero de 2018, http://krebsonsecurity.com/2017/01/who-is-anna-senpai -el-gusano-mirai-autor.

13. Urban Dictionary, s.v. "Swatting", por Droct, 27 de agosto de 2014, http://urbandictionary.com/define.php?term=Swatting.

14. Lewis, "Impacto económico de la ciberdelincuencia".

15. Krebs, "Quién es Anna-Senpai".

16. Departamento de Comercio de Estados Unidos, Departamento de Seguridad Nacional de Estados Unidos, "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats", 22 de mayo de 2018, http://commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

17. CBL (Composite Blocking List), "CBL Breakdown by Country, Highest by Count", Spamhaus, consultado el 24 de abril de 2018, http://abuseat.org/public/country.html.

18. Instituto CyberGreen (sitio web), consultado el 21 de mayo de 2018, http://cybergreen.net.

19. Véase Richard Haass, *A World in Disarray: American Foreign Policy and the Crisis of the Old Order* (Nueva York: Penguin Press, 2017).

20. Jason Healey y Hannah Pitts señalan que esta tensión entre la soberanía del Estado y la obligación internacional se ha abordado en el derecho ambiental internacional "a través de la articulación de la responsabilidad limitada del Estado por ciertos actos que se originan en el territorio de un Estado y que causan daño a otro Estado o a sus ciudadanos". Jason Healey y Hannah Pitts, "Applying International Environmental Legal Norms to Cyber Statecraft,"

21. *I/S: A Journal of Law and Policy for the Information Society* 8, nº 2 (2012).

El principio de la obligación soberana está representado en el derecho ambiental por casos como el de la Fundición Trail, en el que una disputa transfronteriza entre Estados Unidos y Canadá relacionada con la contaminación contribuyó a establecer el principio de que los Estados tienen la obligación, en virtud del derecho internacional, de evitar daños a sus vecinos. Véase Catherine Prunella,
"Un estudio de caso de derecho ambiental internacional: El arbitraje de la fundición de Trail". *Cuestiones de contaminación internacional*, diciembre de 2014, http://intlpollution.commons.gc.cuny.edu /un-estudio-de-caso-de-derecho-ambiental-internacional-el-arbitraje-del-suelo.

22. Departamento de Comercio de los Estados Unidos, Departamento de Seguridad Nacional de los Estados Unidos, "A Report to the President".

23. Estas recomendaciones se basan en el trabajo de I Am the Cavalry, una organización sin ánimo de lucro dedicada a mejorar la seguridad de los dispositivos del IoT. Véase http://iamthecavalry.org; para
Para un análisis más completo, véase "Mejora de la resistencia de Internet": "Acción 1.1. Utilizando procesos inclusivos liderados por la industria, establecer líneas de base de capacidades de IoT aplicables internacionalmente que apoyen la seguridad del ciclo de vida de las aplicaciones domésticas e industriales fundadas en normas internacionales voluntarias e impulsadas por la industria."

24. "Consumer Reports lanza un estándar digital para salvaguardar la seguridad y la privacidad de los consumidores en un mercado complejo", comunicado de prensa, *Consumer Reports* Media Room, 6 de marzo de 2017, http://consumerreports.org/media-room/press-releases/2017/03 /informes_del_consumidor_lanza_el_estándar_digital_para_proteger_la_seguridad_del_consumidor _y_la_privacidad_en_el_mercado_complejo.

25. Spamhaus Malware Labs, "Spamhaus Botnet Threat Report 2017", Spamhaus, 1 de enero de 2018, http://spamhaus.org/news/article/772/spamhaus-botnet-threat -informe-2017.

26. Kathleen Richards, "Botnet Takedowns: Una defensa dramática", *Search Security* (blog), TechTarget, marzo de 2013, https://searchsecurity.techtarget.com/feature/Botnet -Toma de contacto -Defensa dramática.

27. Jason Healey, "Innovación en la colaboración cibernética: Leverage at Scale", Atlantic Council, mayo de 2018, http://atlanticcouncil.org/images/publications/Innovation-Cyber -WEB.pdf.

28. Ibid.

SOBRE LOS AUTORES

Jason Healey es un investigador senior de la Escuela de Asuntos Internacionales y Públicos de la Universidad de Columbia, especializado en conflictos, competencia y cooperación cibernéticos. Anteriormente, fue el director fundador de la Cyber Statecraft Initiative en el Atlantic Council, donde sigue siendo miembro senior. Ha trabajado para Goldman Sachs, incluso como director ejecutivo en Hong Kong. Como director de protección de la ciberinfraestructura en la Casa Blanca de 2003 a 2005, asesoró al Presidente George W. Bush y coordinó los esfuerzos de Estados Unidos para proteger el ciberespacio y las infraestructuras críticas. De 2001 a 2003 fue vicepresidente del Centro de Análisis e Intercambio de Información de Servicios Financieros. Healey comenzó su carrera en las Fuerzas Aéreas de EE.UU., obteniendo dos medallas al mérito por su trabajo inicial en operaciones cibernéticas en el cuartel general de las Fuerzas Aéreas en el Pentágono y como miembro fundador de la Joint Task Force-Computer Network Defense, la primera unidad conjunta de lucha cibernética del mundo. Ha sido profesor de ciberpolítica en la Universidad de Georgetown y de estudios de ciberseguridad nacional en la Escuela de Estudios Internacionales Avanzados de la Universidad Johns Hopkins.

Healy es el editor de *A Fierce Domain: Cyber Conflict, 1986 to 2012* y coautor de *Cyber Security Policy Guidebook*. Sus artículos y ensayos han sido publicados por think tanks como el Aspen Strat- egy Group, el Atlantic Council y el National Research Council, y por revistas académicas de las universidades de Brown y Georgetown, entre otras. Es miembro del Defense Science Board Task Force on Cyber Deterrence y presidente de la Cyber Conflict Studies Association. Healy es licenciado en Ciencias Políticas por la Academia de las Fuerzas Aéreas de EE.UU., en Artes Liberales por la Universidad Johns Hopkins y en Seguridad de la Información por la Universidad James Madison.

Robert K. Knake es investigador principal de ciberpolítica en el Consejo de Relaciones Exteriores (CFR). También es investigador científico senior en el Instituto de Resiliencia Global de la Universidad Northeastern. Knake trabajó de 2011 a 2015 como director de política de ciberseguridad en el Consejo de Seguridad Nacional. En este puesto, fue responsable del desarrollo de la política presidencial en materia de ciberseguridad y construyó y gestionó procesos federales para la respuesta a incidentes cibernéticos y la gestión de la vulnerabilidad. Antes de incorporarse al gobierno, Knake fue becario de asuntos internacionales en el CFR.

Entre las publicaciones de Knake se encuentran *Cyber War: The Next Threat to National Security and What to Do About It (Ciberguerra: la próxima amenaza para la seguridad nacional y qué hacer al respecto)* y el informe especial del Consejo CFR *Internet Governance in an Age of Cyber Insecurity (Gobernanza de Internet en la era de la ciberinseguridad)*. Ha testificado ante el Congreso sobre el intercambio de información en materia de ciberseguridad y sobre el problema de la atribución en el ciberespacio, y ha escrito y dado numerosas conferencias sobre política de ciberseguridad. Knake es licenciado en historia y gobierno por el Connecticut College y tiene un máster en política pública por la Harvard Kennedy School.

COMITÉ CONSULTIVO
Cero botnets

David Altshuler
TechFoundation

Chris B. Baker
Dyn Inc.

Chris Boyer
AT&T

Fred H. Cate
Universidad de Indiana

Benjamin Dean
Iconoclasta Tech LLC

Matthew Eggers
Cámara de Comercio de Estados Unidos

Kristen E. Eichensehr
Facultad de Derecho de la Universidad de California, Los Ángeles

Ben Flatgard
JP Morgan Chase & Co.

Margie Gilbert
Equipo Cymru, Inc.

Ryan M. Gillis
Palo Alto Networks

Nathaniel J. Gleicher
Facebook

Brittan Heller
Liga Antidifamación

Cameron F. Kerry
Institución Brookings

Jongsun A. Kim
Comité Selecto de Inteligencia del Senado de los Estados Unidos

Douglas J. Kramer
Cloudflare, Inc.

Michael Kuiken
Oficina del senador Charles Schumer

Este informe refleja las opiniones y recomendaciones de los autores. No representa necesariamente las opiniones de los miembros del comité consultivo, cuya participación no debe interpretarse en modo alguno como una aprobación del informe por parte de ellos mismos o de las organizaciones a las que están afiliados.

Cover photo: Empty cabinets in the data center of T-Systems, the largest German information technology company, on July 1, 2014, in Biere, Germany.
(Thomas Trutschel/Photothek via Getty Images)

Council on Foreign Relations
www.cfr.org

58 East 68th Street
New York, NY 10065
tel 212.434.9400

1777 F Street, NW
Washington, DC 20006
tel 202.509.8400