Libro blanco técnico del sector

17 de julio de 2017

RESUMEN

El 11 de mayo de 2017, el presidente Trump firmó la Orden Ejecutiva 13800, Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica, encargando al Departamento de Comercio y al Departamento de Seguridad Nacional que lideren un proceso abierto y transparente para identificar formas de mejorar la resiliencia del ecosistema de Internet y las comunicaciones y reducir las amenazas perpetuadas por las botnets, en particular los ataques de denegación de servicio distribuidos. En este libro blanco técnico, el sector de las comunicaciones describe el problema de las redes de bots desde la perspectiva de los proveedores de servicios de Internet (ISP), identifica algunos retos y oportunidades y, a continuación, propone varias recomendaciones preliminares o medidas prácticas que los participantes en el ecosistema, incluidos los ISP, deberían considerar para mitigar las amenazas asociadas a las redes de bots y los ataques automatizados.

Consejo de Coordinación del Sector de las Comunicaciones

Índice de contenidos

Resumen ejecutivo

Un bot es un código utilizado para hacerse con el control de un ordenador o un dispositivo para formar una red de máquinas infectadas, conocida como botnet. Muchas redes de bots son redes autodifusoras y autoorganizadas de máquinas comprometidas que pueden utilizarse para realizar actividades maliciosas de forma coordinada a través de canales de mando y control (C&C). Aunque los bots no son nuevos, el creciente despliegue de dispositivos de la Internet de las Cosas (IoT) amplifica su capacidad para crear una amenaza de seguridad global a gran escala.

En reconocimiento de esta creciente amenaza global, el 11 de mayo de 2017, el presidente Trump firmó la Orden Ejecutiva 13800, *Fortalecimiento de la Ciberseguridad de las Redes Federales y la Infraestructura Crítica,*[1] encargando al Departamento de Comercio (DoC) y al Departamento de Seguridad Nacional (DHS) que lideren un proceso abierto y transparente para identificar formas de mejorar la resiliencia del ecosistema de Internet y las comunicaciones y reducir las amenazas perpetuadas por bots y redes de bots.

En este libro blanco técnico, el sector de las comunicaciones, concretamente los proveedores de servicios de Internet (PSI) en este contexto, pretende informar sobre ese proceso describiendo las responsabilidades compartidas de los principales participantes en el ecosistema de Internet para mitigar las amenazas que suponen las redes de bots. Es una falacia creer que un solo componente del ecosistema de Internet tiene la capacidad de mitigar la amenaza de los botnets y otros sistemas automatizados. Si bien los ISP, como propietarios y operadores de infraestructuras, desempeñan un papel importante en este ecosistema, también lo hacen los fabricantes de dispositivos, los desarrolladores de software, los integradores de sistemas, los proveedores de bordes, los proveedores de servicios en la nube y otros. Será necesario el esfuerzo concertado de todos los miembros de este ecosistema para hacer frente plenamente a las amenazas de los bots y las redes de bots.

El ecosistema de Internet lleva años trabajando en colaboración para neutralizar las amenazas de los bots y las redes de bots. En este documento, el Consejo de Coordinación del Sector de las Comunicaciones (CSCC) identifica una serie de retos para mitigar las redes de bots y las oportunidades para aumentar la colaboración y la cooperación entre los miembros del ecosistema de Internet para abordar el problema, incluyendo:

- Mejorar la eficacia del proceso de aplicación de la ley para acabar con las redes de bots;

[1] Oficina del Secretario de Prensa de la Casa Blanca, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (11 de mayo de 2017), disponible en https://www.whitehouse.gov/the-press- office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

- Intercambio de información procesable sobre ciberamenazas;
- Reducir la dependencia del uso de las funciones de traducción de direcciones de red (NAT);
- Mitigación del tráfico de botnets procedente de países extranjeros;
- Gestionar las notificaciones de los usuarios finales sobre las infecciones de malware;
- Defensa contra dispositivos IoT no seguros;
- Combatir el uso del servidor de nombres de dominio (DNS) de flujo rápido por parte de las redes de bots para ocultar su infraestructura; y
- Coordinar la gestión de la red entre redes.

Como parte del proceso abierto y transparente del DoC y el DHS, el CSCC también propone las siguientes recomendaciones preliminares o pasos accionables que los participantes del ecosistema, incluidos los ISP, deberían considerar para mitigar las amenazas asociadas con los bots, las redes de bots y los ataques automatizados:

- Agilizar el proceso de aplicación de la ley para acabar con las redes de bots;
- Fomentar la migración continua a IPv6;
- Garantizar que la información sobre ciberamenazas que se comparte es procesable y está adaptada a las necesidades de los destinatarios;
- Los operadores de redes y los usuarios finales deberían incluir disposiciones prenegociadas para el filtrado del tráfico en los acuerdos de tránsito y de interconexión;
- Animar a la Corporación de Asignación de Nombres y Números de Internet (ICANN), a los registros y a los registradores a adoptar las técnicas de mitigación de flujo rápido recomendadas por el Comité Asesor de Seguridad y Estabilidad (SSAC);
- Mejorar la detección de botnets fomentando la adopción y el uso de técnicas de aprendizaje automático;
- Asegúrese de que todos los puntos finales, incluidos los dispositivos IoT, cumplen las normas de seguridad desarrolladas por el sector;
- Asegurarse de que los puntos finales ejecutan software actualizado; y
- Los dispositivos IoT deben utilizar técnicas de aislamiento de la red y/o de filtrado basado en la red para cualquier comunicación con los servicios basados en la nube.

Ecosistema de Internet y sector de las comunicaciones

El ecosistema que sustenta Internet, incluidos los miembros del sector de las comunicaciones que prestan servicios de acceso a Internet, es complejo, diverso e interdependiente. Para comprender plenamente las amenazas que plantean las redes de bots, es importante entender el ecosistema y las relaciones entre las partes interesadas. Esta sección ofrece un resumen del ecosistema de Internet y explica cómo encaja el sector de las comunicaciones en el ecosistema más amplio de Internet para proteger las infraestructuras críticas de las amenazas de los bots y las redes de bots.

Ecosistema de Internet

El ecosistema de Internet es un sistema diverso y muy integrado, compuesto por muchas partes interesadas. La Internet Society (ISOC) describe el amplio ecosistema de Internet como compuesto por seis comunidades principales, tal y como se muestra a continuación. [2]

[2] Internet Society, *Who Makes the Internet Work: The Internet Ecosystem* (3 de febrero de 2014), disponible en http://www.internetsociety.org/who-makes-internet-work-internet-ecosystem (consultado el 16 de julio de 2017).

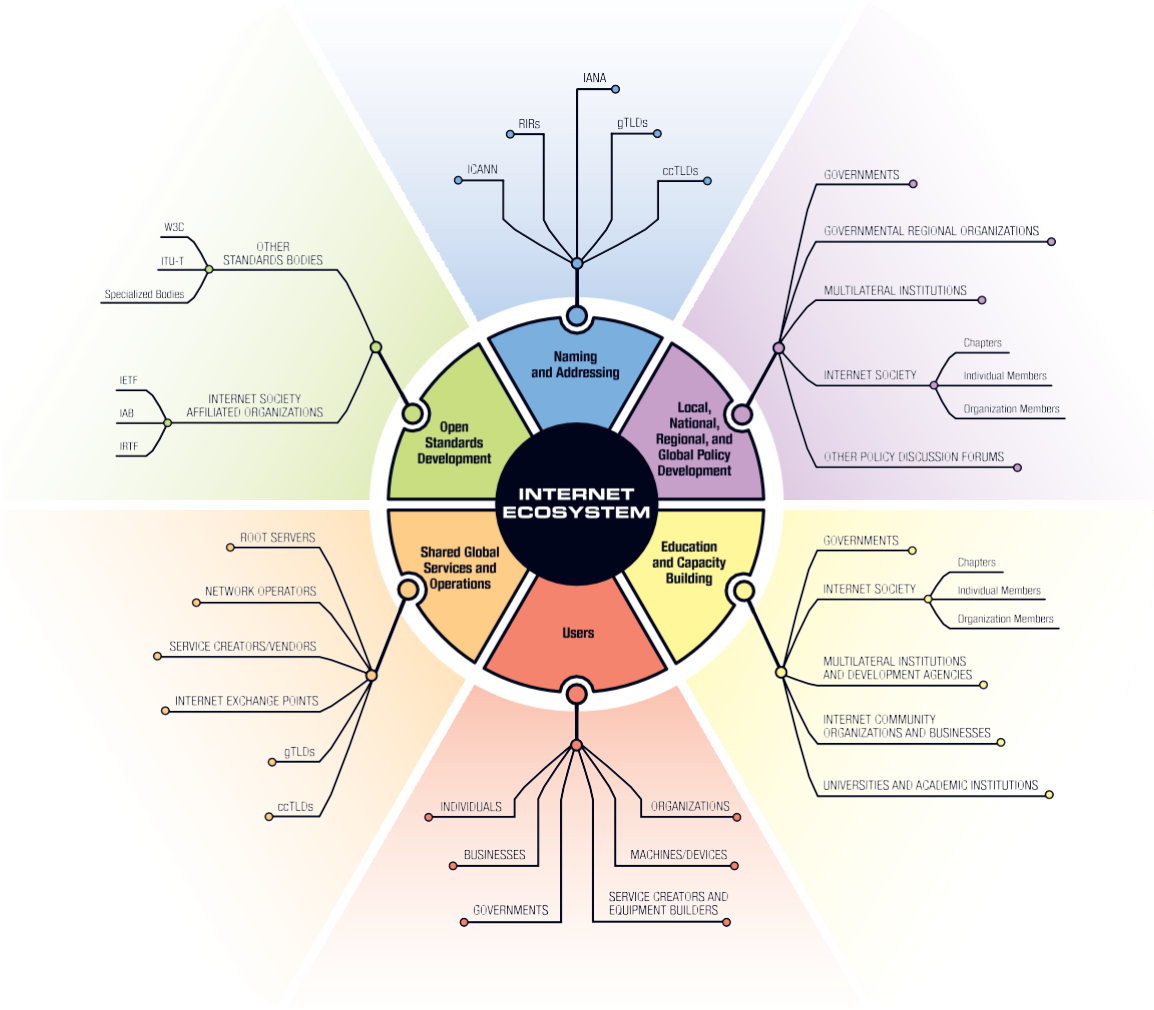

Figura 1 Ecosistema de Internet Fuente:

Internet Society

Los operadores de red, que forman parte del sector de las comunicaciones, proporcionan los "Servicios y Operaciones Globales Compartidos" que se muestran en la Figura 1. Visto únicamente desde la perspectiva de la red, el ecosistema de Internet se parece más a la figura 2.

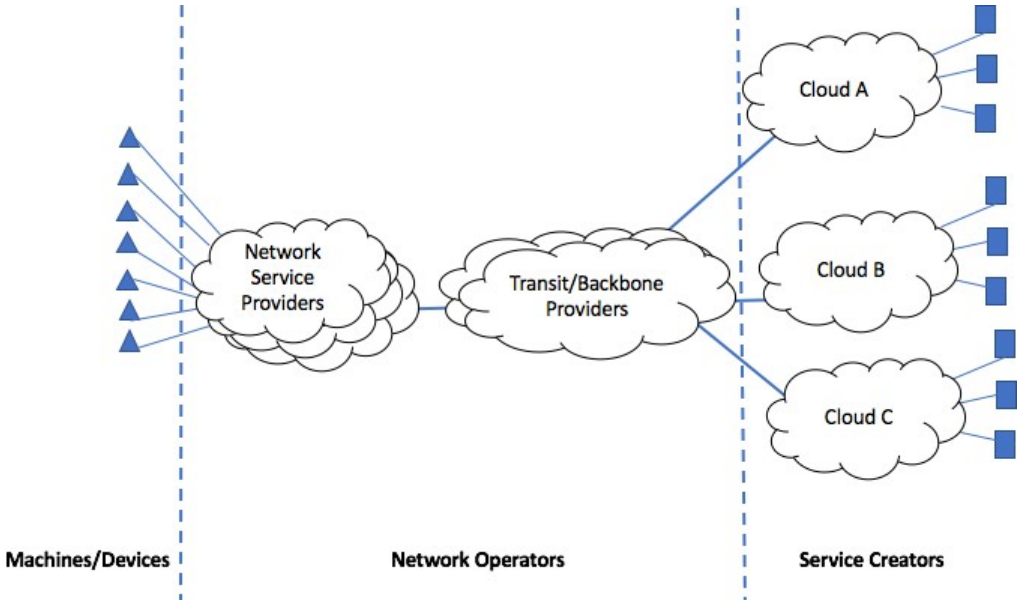

Figura 2 Vista en red del ecosistema de Internet

En este contexto, el ecosistema de internet se compone de muchas máquinas/dispositivos (por ejemplo, smartphones, ordenadores de sobremesa, dispositivos IoT, etc.) que se conectan a los proveedores de servicios de red. Los proveedores de servicios de red utilizan una combinación de tránsito y peering3 para proporcionar conectividad a Internet a los creadores de servicios (por ejemplo, alojamiento, comercio electrónico, medios sociales, empresas, etc.).

Muchos de los creadores de servicios están basados en la nube, lo que significa que operan una red de máquinas que trabajan juntas para proporcionar un servicio. Todas las partes trabajan juntas para proporcionar lo que comúnmente se conoce como Internet.

Sector de las comunicaciones

Los propietarios y operadores de la infraestructura de comunicaciones (radiodifusión, cable, satélite, inalámbrica y alámbrica) conforman el sector de las comunicaciones. El sector de las comunicaciones es uno de los 16 sectores de infraestructuras críticas/recursos clave (CI/KR) identificados en el Plan Nacional de Protección de Infraestructuras (NIPP) del DHS. Este sector incluye a los operadores de redes que proporcionan servicios de acceso a Internet. En el marco de una asociación público-privada con el DHS, el sector de las comunicaciones utiliza el Consejo de Coordinación del Sector de las Comunicaciones (CSCC) y el Centro de Información de las Comunicaciones.

[3] Nota: En el Apéndice B hay un glosario que proporciona más información sobre los términos técnicos utilizados en este documento.

Sharing and Analysis Center (Comm-ISAC) para ayudar a proteger las redes de comunicaciones CI/KR de cualquier daño.

El sector de las comunicaciones tiene una larga historia de cooperación entre sus miembros y con el gobierno federal con respecto a la seguridad nacional y la preparación para emergencias. Esta historia distingue al sector de las comunicaciones de la mayoría de los otros sectores críticos identificados en el Plan Nacional de Protección de Infraestructuras (NIPP). El sector es un ejemplo de cooperación y relaciones de confianza que han dado lugar a la prestación de servicios críticos cuando se producen emergencias y desastres. Este fuerte vínculo existe en gran medida gracias a tres organizaciones que se han creado en respuesta a anteriores amenazas a las infraestructuras críticas de la nación.

Política - El Comité Asesor de Telecomunicaciones de Seguridad Nacional (NSTAC). El NSTAC (wwwncs.gov/nstac/nstachtml) fue creado en 1982 por la Orden Ejecutiva 12382. Se puede consultar en constituye un ejemplo de gran éxito de cómo la industria ayuda a dirigir las decisiones del gobierno en torno a las comunicaciones de seguridad nacional y preparación para emergencias (NS/EP). El NSTAC está formado por hasta 30 directores ejecutivos de las principales empresas de telecomunicaciones, proveedores de servicios de red y empresas de tecnología de la información, financieras y aeroespaciales. A través de un proceso deliberativo, proporcionan al Presidente recomendaciones destinadas a asegurar los enlaces vitales de telecomunicaciones a través de cualquier evento o crisis, y para ayudar al Gobierno de Estados Unidos a mantener una postura de comunicaciones nacionales fiables, seguras y resistentes. Las principales áreas de interés del NSTAC son: el fortalecimiento de la seguridad nacional, la mejora de la ciberseguridad, el mantenimiento de la infraestructura global de comunicaciones, la garantía de las comunicaciones para la respuesta a las catástrofes y el tratamiento de las interdependencias de las infraestructuras críticas.

Planificación - Consejo de Coordinación del Sector de las Comunicaciones (CSCC). El CSCC se constituyó en 2005 para ayudar a coordinar las iniciativas destinadas a mejorar la seguridad física y cibernética de los activos del sector; facilitar el flujo de información dentro del sector, entre sectores y con los organismos federales designados; y abordar las cuestiones relacionadas con la respuesta y la recuperación tras un incidente o evento. Los más de 40 miembros del CSCC representan ampliamente al sector e incluyen proveedores de cable, emisoras comerciales y públicas, proveedores de servicios de información, proveedores de satélite, proveedores de cable submarino, proveedores de telecomunicaciones de servicios públicos, integradores de servicios, proveedores de equipos y propietarios y operadores de redes inalámbricas y de cable y sus respectivas asociaciones comerciales.

Operaciones - Centro Nacional de Coordinación de Telecomunicaciones (NCC)

Centro de Análisis e Intercambio de Información de Comunicaciones (Comm-ISAC). En 1982, funcionarios del gobierno federal y de la industria de las telecomunicaciones identificaron la necesidad de un mecanismo conjunto para coordinar el inicio y el restablecimiento de los servicios de telecomunicaciones de seguridad nacional y de preparación para emergencias. En 1984, la Orden Ejecutiva 12472 creó el NCC. La asociación única de esta organización entre la industria y el gobierno avanza en la colaboración en cuestiones operativas sobre una base de 24 X 7 y coordina las respuestas NS/EP en tiempos de crisis. Desde el año 2000, el Centro de Análisis e Intercambio de Información sobre Comunicaciones (Comm-ISAC) del NCC, compuesto por 51 empresas miembros de la industria, ha facilitado el intercambio de información entre los participantes del gobierno y de la industria en relación con las vulnerabilidades, amenazas, intrusiones y anomalías que afectan a la infraestructura de telecomunicaciones. Los representantes de la industria y del gobierno se reúnen semanalmente para compartir información sobre amenazas e incidentes. Durante las emergencias, los representantes de la industria y del gobierno que participan en los esfuerzos de respuesta se reúnen diariamente, o incluso con mayor frecuencia.

Bots, botnets y amenazas asociadas

> *Bot - un programa que se instala en un sistema para permitir que ese sistema realice automáticamente (o semiautomáticamente) una tarea o conjunto de tareas, normalmente bajo el mando y control de un administrador remoto (también conocido como bot master o bot herder).* [4]
>
> *Botnet: una red de dispositivos informáticos de usuario final conectados a Internet, infectados con malware bot y controlados remotamente por terceros con fines nefastos.* [5]

Los bots no son un fenómeno nuevo. Es importante señalar que no todos los bots son malos, y que no todas las redes de bots se utilizan con fines nefastos. Hay algunos bots buenos en entornos como los juegos y el Internet Relay Chat (IRC). Sin embargo, a efectos de este documento, todas las menciones a los bots y a las redes de bots supondrán que son de naturaleza maliciosa o potencialmente maliciosa.

Una "botnet" es una red de bots que trabajan juntos con la capacidad de actuar según las instrucciones generadas de forma remota. Una red de bots típica puede tener desde unos pocos miles de bots hasta cientos de

---

[4] Comisión Federal de Comunicaciones (FCC), Communications Security Reliability and Interoperability Council (CSRIC) III, *U.S. Anti- Bot Code of Conduct (ABCs) for Internet Service Providers*, (Mar. 2012), disponible en https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf (consultado el 20 de junio de 2017).

[5] *Id.*

miles o incluso millones de bots. Los bots y las redes de bots son altamente personalizables y pueden ser programados para hacer muchas cosas, incluyendo: el robo de información personal y otra información sensible, el spam, la recolección de direcciones de correo electrónico, los ataques de denegación de servicio distribuidos (DDoS), el registro de claves, el alojamiento de contenido ilegal y el fraude por clic. Estos tipos de ciberataques se describen con más detalle más adelante en este documento.

Los primeros bots utilizaban el IRC para comunicarse con sus servidores de C&C. Con el tiempo, los bots y las redes de bots se han vuelto más sofisticados. Por ejemplo, los bots y las redes de bots se han hecho más resistentes al incorporar arquitecturas y protocolos peer-to-peer (P2P); algoritmos de generación de nombres de dominio; protocolo de transferencia de hipertexto (HTTP) a localizadores uniformes de recursos (URL) específicos dentro de sitios web legítimos; infraestructuras de C&C sofisticadas y jerárquicas; y cifrado. Cada una de estas mejoras ha hecho más difícil identificar y aislar el tráfico malicioso del tráfico legítimo de la red.

Históricamente, los bots infectaban los ordenadores de sobremesa y los servidores, lo que provocaba su detección y eliminación mediante software antivirus. En cambio, los dispositivos IoT no suelen tener una interfaz de usuario (UI), están diseñados para funcionar de forma autónoma y están conectados directa o indirectamente a Internet. Estos dispositivos no se prestan a algunas protecciones de seguridad tradicionales. Pueden conectarse a Internet sin un cortafuegos y suelen estar situados en el mismo segmento de red de área local (LAN) que otros objetivos de mayor valor. Es poco probable que ejecuten software antivirus. Además, pueden considerarse un riesgo de seguridad bajo, ya que son de bajo coste y sólo procesan datos aparentemente inocuos. Sin embargo, los dispositivos IoT son en realidad objetivos tentadores para la explotación, ya que los dispositivos proporcionan una potencia de cálculo que puede ser utilizada por los malos actores, normalmente sin que los propietarios se den cuenta, y a menudo son equipos de "instalar y olvidar".

Las grandes redes de dispositivos IoT pueden verse comprometidas por bots cuando se conectan a conexiones de Internet de alta velocidad, lo que puede causar daños importantes. El ataque DDoS de la red de bots Mirai de octubre de 2016 contra el proveedor de DNS Dyn es uno de los ejemplos más recientes. La red de bots Mirai se aprovechó de la débil seguridad de muchos dispositivos IoT escaneando continuamente Internet, en busca de más dispositivos IoT que estuvieran protegidos por nombres de usuario y contraseñas predeterminados o codificados. [6] A medida que la red de bots Mirai descubría dispositivos IoT vulnerables, cargaba su malware en los dispositivos y comenzaba a comunicarse con los servidores de C&C en espera de instrucciones. A continuación, la red de bots Mirai

---

6 Symantec Security Response, *Mirai: what you need to know about the botnet behind recent major DDoS attacks*, Symantec Official Blog (27 de octubre de 2016), disponible en https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind- recent-major-ddos-attacks (consultado el 20 de junio de 2017).

utilizado para lanzar un ataque DDoS a gran escala contra Dyn, instruyendo a cada dispositivo infectado para que inundara los servidores DNS de Dyn con un gran volumen de paquetes utilizando el puerto de destino del servicio DNS (protocolo de datagramas de usuario (UDP) puerto 53), además de inundar los servidores autoritativos con numerosas solicitudes de nombres de dominio no válidos. [7] El ataque impidió que varios clientes de Dyn pudieran acceder a los nombres de dominio servidos por Dyn DNS durante el ataque.

El ataque a Dyn no fue un incidente aislado. El tamaño máximo del ataque aumentó drásticamente en un corto período de tiempo, pasando de 500 Gbps en 2015 a 800 Gbps en 2016.[8] El sitio KrebsonSecurity también sufrió un ataque en septiembre de 2016, que alcanzó los 620 Gbps. De hecho, la red de bots Mirai y otras redes de bots de IoT existían desde algún tiempo antes de estos ataques y generalmente se utilizaban para realizar ataques DDoS más pequeños.

Amenazas de botnets

Como se ha descrito anteriormente, los bots y las redes de bots son altamente personalizables, y como resultado, pueden ser programados para hacer muchas cosas beneficiosas en Internet. Sin embargo, a menudo y cada vez más, se utilizan para actividades nefastas como los tipos de ataques que se enumeran a continuación.

- Ataques DDoS;
- Robo de datos;
- Distribución de contenidos ilícitos;
- Adivinación de contraseñas por fuerza bruta;
- Procesando el robo;
- Fraude por clic;
- Spam por correo electrónico; y
- Pasarela no autorizada.

El resto de esta sección, sin embargo, se centrará en los ataques DDoS. En el Apéndice B se pueden encontrar descripciones de los otros tipos de ataques enumerados anteriormente.

---

[7] Scott Hamilton, *Dyn Analysis Summary Of Friday October 21 Attack*, Dyn Blog (26 de octubre de 2016), disponible en http://dyn.com/blog/dyn- analysis-summary-of-friday-october-21-attack/ (consultado el 20 de junio de 2017).
[8] Arbor Networks, *12th Annual Worldwide Infrastructure Security Report*, Arbor Networks Special Report Vol. XII (2016), en la página 21, disponible en https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf (consultado el 30 de junio de 2017).

Los ataques DDoS -una forma muy frecuente de ataque perpetrado por redes de bots- ilustran algunos de los muchos retos que plantea la prevención de los ataques, así como evitar que los bots pongan en peligro los puntos finales.

Los ataques DDoS pueden dividirse en cuatro categorías principales:[9]

- Volumétrico;
- Aplicación/recursos;
- El agotamiento del Estado; y
- Plano de control.

Los ataques DDoS volumétricos consisten en cientos o cientos de miles de bots que inundan a la víctima con paquetes, provocando la denegación del servicio a otros. Los ataques pueden ser directos, en los que los bots envían los paquetes dirigidos directamente a la víctima, ya sea con su propia dirección IP de origen o con una dirección IP de origen falsa. Los ataques indirectos aprovechan una técnica conocida como ataque de amplificación reflexiva, en la que los bots falsean la dirección IP de origen para que sea la del objetivo del ataque. [10] A continuación, los bots envían paquetes de solicitud a otros servicios como DNS, Character Generator Protocol (chargen) o Simple Service Discovery Protocol (SSDP) para engañar a los servicios para que envíen respuestas hacia la víctima. Los ataques indirectos o de reflexión suelen estar diseñados para hacer que el servicio envíe una respuesta mucho mayor que la solicitud inicial del bot, lo que da lugar a un ataque de amplificación. En algunas circunstancias, las amplificaciones pueden ser miles de veces mayores que los paquetes de solicitud inicial de los bots.

Los ataques a aplicaciones suelen ser ataques de menor volumen de tráfico que los volumétricos. Se caracterizan por el envío por parte de bots de peticiones a nivel de aplicación de apariencia legítima a un sistema para consumir recursos (por ejemplo, CPU, acceso a disco, búsquedas en bases de datos, etc.) y saturar el sistema, impidiendo así que otros accedan a él.

Los ataques por agotamiento del estado aprovechan el hecho de que dispositivos como los servidores, los cortafuegos y los sistemas de detección de intrusos tienen capacidades limitadas para rastrear el estado de las transacciones concurrentes. El sitio web

---

[9] FCC CSRIC IV, *Remediation of Server-Based DDoS Attacks Final Report*, (Sept. 2014), disponible en https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf (consultado el 20 de junio de 2017).

[10] Grupo de Trabajo de Mensajería, Malware y Antiabuso Móvil, *M3AAWG Introduction to Reflective DDoS Attacks* (mayo de 2017), disponible en https://www.m3aawg.org/sites/default/files/m3aawg-reflective-ddos-attack-intro.pdf (consultado el 20 de junio de 2017).

Los bots aprovechan esta limitación y consumen todas las capacidades de estado abriendo muchas conexiones y no continuando completamente esas conexiones hasta su finalización.

Los ataques al plano de control aprovechan las limitaciones de los protocolos de Internet, como el Border Gateway Protocol11 (BGP), IPv6,[12] y el protocolo DNS. [13]

Uno de los retos que plantean todos los tipos de ataques DDoS -especialmente para los ISP- es su identificación. Los ciberdelincuentes están diseñando rápidamente redes de bots más sofisticadas, lo que hace más difícil distinguir el tráfico malo del bueno. Las primeras formas de bots solían transmitir sus mensajes en texto claro, en puertos conocidos, a direcciones IP codificadas, lo que hacía que el tráfico fuera fácil de identificar y bloquear. Cada vez más, los bots enmascaran su tráfico como tráfico a nivel de aplicación (por ejemplo, hacen que parezca tráfico web normal o tráfico web encriptado, utilizan técnicas peer-to-peer para evitar un único punto de fallo, o utilizan VPNs para encriptar y tunelizar su tráfico para evadir la detección).

El ataque de la red de bots Mirai también aprovechó el hecho de que hay millones de dispositivos IoT en todo el mundo, y el tráfico de ataque se generó desde los rincones más lejanos de Internet, con origen en las ubicaciones de las víctimas. Level 3 Threat Research Labs informó de que había observado más de un millón de dispositivos IoT participando en los ataques de redes de bots, y un gran porcentaje se encontraba en Taiwán, Brasil y Colombia. [14] El reto para un ISP a la hora de detectar y bloquear este tráfico es que no se origina en la red del ISP y puede que sólo transite por una parte de la red, si es que lo hace. E incluso si hay bots en la red que originan el tráfico, el volumen de tráfico de los bots puede no ser lo suficientemente alto como para detectarlo en la red.

El tráfico de ataques de botnets puede parecer totalmente normal. Gran parte de él son ataques amplificados reflexivos (que ofrecen la mejor relación calidad-precio), que con frecuencia utilizan servicios comunes bien conocidos como DNS, protocolo de tiempo de red (NTP) y HTTP.

---

[11] K. Butler, et al, *A Survey of BGP Security Issues and Solutions*, Proceedings of the IEEE 98, n.º 1 (enero de 2010), en p. 100-122 (doi:10.1109/jproc.2009.2034031).
[12] Cisco, IPv6 Extension Headers Review and Considerations [IP Version 6 (IPv6)], (10 de octubre de 2006), disponible en http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html(consultado el 30 de junio de 2017).
[13] Suranjith Ariyapperuma, y Chris Mitchell, *Security vulnerabilities in DNS and DNSSec*, Proceedings of Proceedings of The Second International Conference on Availability, Reliability and Security, ARES 2007, The International Dependability Conference - Bridging Theory and Practice, Austria, Viena, disponible en http://web.mit.edu/6.033/www/papers/dnssec.pdf (consultado el 30 de junio de 2017).
[14] Level 3 Research Labs, *Attack of Things!* , disponible en http://www.netformation.com/level-3-pov/attack-of-things-2 (consultado el 20 de junio de 2017).

Hay cientos de tipos diferentes de ataques dentro de las cinco categorías de ataques DDoS. El propio Mirai tiene una docena de ataques DDoS programados. La red de bots se propaga mediante el escaneo de puertos telnet abiertos (protocolo de control de transmisión puerto 23). Telnet es un protocolo de texto claro y es extremadamente inseguro y no debería usarse en Internet, pero así es exactamente como se propagó Mirai. Durante el ataque a Dyn DNS, Mirai utilizó la "tortura del agua" de [DNS15], que proxyó a través de varios resolvedores abiertos conocidos (Google 8.8.8.8, por ejemplo). El ataque al sitio web de KrebsonSecurity16 se diseñó para que pareciera el protocolo de encapsulación de enrutamiento genérico (GRE). [17] Ambos ataques podrían haber sido bloqueados por los proveedores de tránsito de Internet. En el caso del ataque a Dyn, los proveedores de servicios de red y el Comm-ISAC se pusieron en contacto con Dyn para ofrecerle ayuda.

El ataque de KrebsonSecurity, al estar basado en GRE, podría haber sido bloqueado por la mayoría de los ISP. El tráfico de Dyn estaba proxyado por resolvedores abiertos bien conocidos, por lo que la limitación de la tasa de ese tráfico hacia las IP de Dyn podría haber mitigado la mayor parte de los efectos de ese ataque. Brobot, que afectó a muchos sistemas financieros estadounidenses, utilizó HTTP y HTTPS para la mayoría de sus ataques. Para bloquearlo sería necesario examinar y filtrar el contenido, algo que los ISP no suelen hacer y no pueden hacer para HTTPS sin tener las claves privadas del usuario final. El tráfico malicioso que está cifrado (por ejemplo, HTTPS) no puede filtrarse.

Los últimos ataques ilustran la sofisticación y la escala que han alcanzado las redes de bots. Las redes de bots son detectables; el reto es detenerlas. La mejor manera de detenerlas es evitar su propagación en primer lugar. El verdadero reto para el ecosistema de Internet a la hora de hacer frente a las amenazas de las redes de bots es la reparación de los puntos finales infectados. Si no se remedia el punto final o se desconecta el punto final infectado de Internet, la amenaza del punto final infectado permanece. Garantizar que los puntos finales ejecuten el software más reciente con los últimos parches de seguridad es una práctica recomendada reconocida para mitigar la propagación y las amenazas de los bots maliciosos y nefastos.

---

[15] La tortura de agua DNS es un tipo de ataque en el que muchos puntos finales envían consultas para el dominio de una víctima con una cadena aleatoria añadida al dominio que sobrecarga el servidor DNS autoritativo de la víctima y hace que el dominio de la víctima sea inaccesible.

[16] *Véase,* https://krebsonsecurity.com.

[17] KrebsonSecurity, *KrebsOnSecurity Hit With Record DDoS* (21 de septiembre de 2016), disponible en http://krebsonsecurity.com/tag/gre-ddos/ (consultado el 16 de julio de 2017).

La mayor parte del tráfico de botnets se origina fuera de Estados Unidos

El panorama de las amenazas de las redes de bots sigue evolucionando. Según las empresas de inteligencia de amenazas, las tendencias notables identificadas en el panorama de las amenazas en 2016 son que: 1) los dispositivos IoT inseguros son una gran fuente de tráfico de ataques DDoS; [18] y 2) la gran mayoría del tráfico de ataques se origina fuera de Estados Unidos. [19]

En 2016, los ataques desde dispositivos IoT fueron noticia con los ataques de la red de bots Mirai desde cámaras de seguridad mal protegidas y sus grabadores de circuito cerrado de televisión (DVR). Como señaló Level 3 Threat Research Labs, muchas de las cámaras y DVR inseguras se encontraban en Taiwán, Brasil y Colombia. [20] Shodan[21] , un motor de búsqueda que permite al usuario encontrar tipos específicos de dispositivos IoT y de otro tipo que están conectados y son visibles en la Internet pública, informa (a partir de julio de 2017) de más de 300.000 dispositivos Hikvision susceptibles de ser conectados directamente a la Internet, con la gran mayoría de esos dispositivos ubicados en Brasil (45.000), India (36.000), China (34.000), México (25.000) y Sudáfrica. Corea (20.000). [22]

Aunque es difícil atribuir el origen exacto de los ataques de redes de bots, casi siempre es posible determinar el país de origen del tráfico. Numerosos informes23 indican que las principales fuentes de tráfico de ataques son China y otros países del sudeste asiático (por ejemplo, Vietnam, Taiwán y Tailandia). [24]

Esto coincide con un estudio anterior que mostraba una fuerte correlación entre los dispositivos utilizados para los ataques de redes de bots y el país en el que residen los dispositivos. Estos dispositivos suelen ejecutar software sin los últimos parches de seguridad. [25] En un estudio, los investigadores analizaron seis

---

[18] Akamai, *Informe sobre el estado de la seguridad en Internet del cuarto trimestre de 2016* (invierno de 2016), disponible en https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (consultado el 20 de junio de 2017).
[19] Incapsula.com, *Global DDoS Threat Landscape Q1 2017* (primavera de 2017), disponible en https://www.incapsula.com/ddos-report/ddos- report-q1-2017.html (consultado el 20 de junio de 2017).
[20] Level 3 Research Labs, *Attack of Things!* , disponible en http://www.netformation.com/level-3-pov/attack-of-things-2 (consultado el 20 de junio de 2017).
[21] *Ver* shodan.io (Shodan explora los dispositivos de indexación de Internet que responden a los escaneos de puertos en los puertos 80, 8080, 443, 8443, 21, 22,23,161, 5060, 554 y otros puertos conocidos).
[22] Shodan, búsqueda de "Hikvision", disponible en https://www.shodan.io/search?query=hikvision (consultado el 20 de junio de 2017).
[23] *Véase en* el Apéndice A de este documento los datos de diferentes informes sobre amenazas.
[24] Incapsula.com, *Global DDoS Threat Landscape Q1 2017* (primavera de 2017), disponible en https://www.incapsula.com/ddos-report/ddos- report-q1-2017.html (consultado el 20 de junio de 2017).
[25] Hadi Asghari, Michael Ciere y Michael J.G. Van Eten, *Post-Mortem of a Zombie: Conficker Cleanup After Six Years*, en USENIX The Advanced Computing Systems Association, Proceedings of 24th USENIX Security Symposium, Washington, D.C. (agosto de 2015), disponible en https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-asghari.pdf (consultado el 20 de junio de 2017).

años de datos longitudinales del sumidero de Conficker, una de las mayores redes de bots jamás vistas, para evaluar el impacto en la mitigación de las redes de bots de las iniciativas nacionales contra las redes de bots, destinadas a conseguir que los usuarios finales limpien las máquinas infectadas. Descubrieron que los niveles máximos de infección están fuertemente correlacionados con la piratería de software. Esto implica que los países con un mayor número de usuarios finales que ejecutan copias de software sin licencia tienden a tener un mayor número de bots porque esos activos tienen un menor porcentaje de usuarios registrados que obtienen parches de seguridad.

Un patrón similar se observó con la red de bots Mirai, que se aprovechó del hecho de que una clase de dispositivos IoT se enviaban con credenciales de inicio de sesión conocidas y predeterminadas que los usuarios finales rara vez cambian.
Las vulnerabilidades de al menos uno de los fabricantes se notificaron ya en 2013.[26] Solo después de que se notificara el ataque a la red de bots Mirai, el fabricante en cuestión proporcionó una actualización del firmware para solucionar las vulnerabilidades, e incluso entonces, se requirió la intervención manual de los usuarios finales de los dispositivos para actualizar el firmware, ya que los dispositivos no admitían una forma automatizada de actualizar su software de forma segura.

Herramientas y técnicas actuales

Aplicación del marco de ciberseguridad contra las redes de bots

El Marco de Ciberseguridad, desarrollado por el Instituto Nacional de Normas y Tecnología (NIST),27 [es] un "conjunto de normas y mejores prácticas de la industria basadas en el riesgo y de carácter voluntario para ayudar a las organizaciones a gestionar los riesgos de ciberseguridad". El Marco se compone de cinco áreas funcionales
– 1) Identificar, 2) Detectar, 3) Proteger, 4) Responder y 5) Recuperar. Los principales ISP utilizan el Marco como parte de sus procesos generales de gestión de riesgos cibernéticos para hacer frente a las amenazas que suponen los bots y las redes de bots contra sus redes.

Identificar

En el Marco, el primer paso es **identificar** tanto lo que hay que proteger como las ciberamenazas. La seguridad de las comunicaciones de la Comisión Federal de Comunicaciones (FCC),

[26] Departamento de Seguridad Nacional (DHS) Oficina de Ciberseguridad y Comunicaciones, *Nota de Vulnerabilidad VU#800094 - Dahua Security DVRs contain multiple vulnerabilities* (4 de diciembre de 2013), disponible en http://www.kb.cert.org/vuls/id/800094 (consultado el 20 de junio de 2017).
[27] National Institute of Standards and Technology, *Cybersecurity Framework* (25 de mayo de 2017), disponible en https://www.nist.gov/cyberframework(consultado el 20 de junio de 2017).

El informe final del Grupo de Trabajo 4 del Consejo de Fiabilidad e Interoperabilidad (CSRIC), *Cybersecurity Risk Management and Best Practices (Gestión de riesgos de ciberseguridad y mejores prácticas*), proporciona orientación sobre el uso del Marco para los proveedores de servicios de red. Los ISP, como parte de la infraestructura crítica, han identificado que necesitan proteger sus redes principales de las amenazas de ciberseguridad como los bots y las botnets. Los ISP también pueden, como parte de un servicio de seguridad gestionado, proteger a sus clientes de los daños de las ciberamenazas.

Además de identificar lo que hay que proteger, los proveedores de servicios de red utilizan el Marco y otras herramientas para identificar las amenazas. El primer paso es identificar las superficies de ataque de los activos que hay que proteger y luego identificar los vectores de ataque conocidos. Esta información se sintetiza continuamente con los datos de inteligencia sobre amenazas para garantizar una cobertura completa e identificar, y en última instancia abordar, nuevas vulnerabilidades. La obtención de datos de alta calidad sobre las ciberamenazas es uno de los aspectos más importantes de la implementación y ejecución de un sólido programa de mitigación de botnets. Para que el programa sea eficaz, es necesario que los datos de falsos positivos sean casi nulos. Los falsos positivos pueden aumentar en gran medida los costes operativos de un proveedor de servicios de red, afectar a la satisfacción de sus clientes y dañar su marca. Como se indica en el informe del Grupo de Trabajo 5 del CSRIC sobre el *intercambio de información sobre* ciberseguridad[28] , los proveedores de servicios de red han desarrollado un ecosistema de intercambio de información para utilizar y compartir la información de los indicadores de ciberamenazas procedente de una serie de fuentes, con el fin de identificar las redes de bots y sus amenazas asociadas. En este ecosistema se incluyen fuentes de datos de terceros de confianza (TTP), información del DHS, incluido su sistema de intercambio de información automatizado (AIS), y el intercambio de información intersectorial.

Detectar

Como se indica en el Marco, la **detección** de amenazas y ataques es el siguiente paso para proteger las redes de los ataques de las redes de bots. Como se ha descrito anteriormente, los ataques de botnets se presentan de muchas formas, por lo que su detección requiere una serie de herramientas y técnicas adaptadas a cada tipo de ataque.
Independientemente del tipo de ataque de la red de bots, los proveedores de servicios de red utilizan un conjunto básico de técnicas, como el muestreo de paquetes, el análisis de firmas y el análisis heurístico o de comportamiento.

Muchas redes de bots intentan disfrazar su tráfico como tráfico normal de Internet. Esto dificulta especialmente la detección de las redes de bots muy distribuidas o de las redes de bots de bajo volumen de tráfico, ya que el

[28] FCC CSRIC V, *Working Group 5: Cybersecurity Information Sharing*, Final Report (15 de marzo de 2017), disponible en https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf (consultado el 20 de junio de 2017).

tráfico estará por debajo de los umbrales de alarma en la red de cualquier operador. Por ejemplo, durante el ataque Mirai Dyn DNS waterboarding, los atacantes proxyaron sus peticiones a través de resolvedores DNS abiertos bien conocidos. [29]

Proteja

Los proveedores de servicios de red utilizan diversas técnicas para **proteger** sus redes de los ataques y adoptan medidas para ayudar a sus clientes a protegerse de los mismos.

Los proveedores de servicios de red utilizan diferentes técnicas de filtrado para proteger directamente su infraestructura de red (por ejemplo, routers, servidores). Los bots suelen falsificar la dirección IP de origen en los paquetes de ataque. Esto se ve típicamente en los ataques de reflexión de red, pero como se ha visto en ataques de gran volumen como la red de bots Mirai o el ataque Dyn, esto se puede lograr incluso sin la suplantación de IP.
En cualquier caso, como mejor práctica común, la mayoría de los proveedores de servicios de red, si no todos, realizan un filtrado de red para las direcciones IP falsas. [30]

Los proveedores de servicios de red también utilizan una combinación de otras técnicas de filtrado, como las listas de control de acceso (ACL), la vigilancia del tráfico, el black holing y el sink holing en sus redes para filtrar el tráfico conocido de las redes de bots. Estas técnicas pueden ser eficaces para neutralizar el tráfico de C&C de las botnets cliente-servidor. Esto es menos eficaz contra las redes de bots más avanzadas que utilizan arquitectura peer-to-peer, cifrado y/o técnicas de DNS de flujo rápido para su canal de C&C. El flujo rápido es una técnica de DNS utilizada por las redes de bots para ocultar los sitios de entrega de phishing y malware detrás de una red siempre cambiante de hosts comprometidos que actúan como proxies.

Los proveedores de servicios de red también han realizado grandes inversiones en sistemas de depuración de DDoS para "depurar" los ataques DDoS contra sus redes y sus clientes que han contratado servicios de mitigación de DDoS. Los sistemas de depuración DDoS se basan en el desvío *del* tráfico de la víctima a través del depurador "a la carta" para filtrar el tráfico de ataque del tráfico bueno, y luego devolverlo a la red del proveedor para enviarlo a su destino original. Los proveedores de servicios de red utilizan una combinación de sistemas de depuración internos y sistemas de depuración de terceros mediante contratos con

---

[29] Scott Hamilton, *Dyn Analysis Summary Of Friday October 21 Attack*, Dyn Blog (26 de octubre de 2016), disponible en http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (consultado el 20 de junio de 2017).
[30] P. Ferguson y D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, Best Current Practice (BCP) 38 (mayo de 2000), disponible en https://tools.ietf.org/html/bcp38 (consultado el 20 de junio de 20170; F. Baker, y P. Savola, *Ingress Filtering for Multihomed Networks*, BCP 84 (marzo de 2004), disponible en https://tools.ietf.org/html/bcp84 (consultado el 20 de junio de 2017); y Mutually Agreed Norms for Routing Security (MANRS), *Participants* (6 de marzo de 2015), disponible en https://www.routingmanifesto.org/participants/(consultado el 20 de junio de 2017).

proveedores de mitigación de DDoS de terceros. Sin embargo, los proveedores de servicios de red *no* tienen la capacidad de depurar todo el tráfico todo el tiempo.

Además de limpiar el tráfico, muchos proveedores utilizan las capacidades Flowspec31 de BGP para bloquear dinámicamente el tráfico fácilmente identificable en el router. El tráfico se suele bloquear utilizando la pareja básica de cinco valores que se encuentra en IPFIX32 (IP de origen y destino, puerto de origen y destino, y protocolo). Flowspec tiene la ventaja de que las actualizaciones de BGP pueden realizarse y retirarse con bastante rapidez en la red, lo que permite una mitigación más rápida.

Los proveedores de servicios de red también pueden proporcionar herramientas y servicios específicos a sus clientes para protegerse, incluyendo software antivirus para puntos finales y puertas de enlace domésticas con seguridad integrada. [33] Los grandes clientes de ISP que operan redes stub o proveedores de borde también pueden utilizar una técnica para mitigar los ataques DDoS conocida como Anycast, que permite que varios hosts o puntos finales tengan la misma dirección IP. Al distribuir geográficamente estos hosts, la magnitud del ataque DDoS tiene que ser significativamente mayor para tener en cuenta los hosts distribuidos y conseguir interrumpir el sitio o el servicio. Los servicios Anycast pueden ser desplegados por los proveedores de borde o comprados a socios de mitigación DDoS.

Varios proveedores de servicios de red también ofrecen un conjunto de servicios de seguridad gestionados que incluyen, entre otros, los servicios de depuración de DDoS mencionados anteriormente. Estos pueden incluir capacidades como cortafuegos basados en la red, servicios de gestión de dispositivos móviles, análisis de amenazas y detección de eventos, conectividad VPN segura a la nube y seguridad web y de correo electrónico.

Responder y recuperar

Hoy en día, como se indica en el Marco de Ciberseguridad, cuando un proveedor de servicios de red detecta tráfico malicioso de un bot en su red o hacia un punto final en su red, **responde y se recupera** según sea necesario. La respuesta consiste en mitigar el impacto del tráfico malicioso y, si es necesario, remediar el punto final infectado.

Para mitigar el tráfico malicioso, el proveedor de servicios de red debe determinar primero el alcance del impacto del tráfico malicioso. Para el tráfico malicioso que afecta a su red o a su

---

[31] Leonardo Serodio, *Traffic Diversion Techniques for DDoS Mitigation using BGP Flowspec* (mayo de 2013), disponible en https://nanog.org/sites/default/files/wed.general.trafficdiversion.serodio.10.pdf (consultado el 7 de julio de 2017).
[32] B. Claise, B. Trammell y P. Aitken, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*, IETF Tools (Sept.2013), disponible en https://tools.ietf.org/html/rfc7011 (consultado el 7 de julio de 2017).
[33] McAfee, *McAfee Web Gateway*, disponible en https://www.mcafee.com/us/products/web-gateway.aspx (consultado el 7 de julio de 2017).

para prestar el servicio, el proveedor de servicios de red tendrá que trabajar para filtrar el tráfico malicioso utilizando una de las técnicas de filtrado (por ejemplo, ACL, agujero negro, agujero de fregado o scrub) descritas anteriormente. Además, si el tráfico malicioso es entrante hacia su red, el proveedor de servicios de red puede ponerse en contacto con la red ascendente y pedirle que filtre el tráfico que emana de esa red.

En el caso del tráfico malicioso que se determina que emana de un punto final del cliente en su red, el proveedor de servicios de red, tal como se recomienda en el Código de Conducta Anti-Bot voluntario para Proveedores de Servicios de Internet (ABC para ISP)[34]:

- **Detectar**: identificar y detectar la actividad de las redes de bots en la red del ISP o en nombre de los clientes empresariales que han contratado los servicios del ISP para determinar posibles infecciones de bots en los dispositivos de los usuarios finales;
- **Notificar** - notificar a los usuarios finales, incluyendo potencialmente tanto a los consumidores como a los clientes empresariales de las sospechas de infecciones de bots;
- **Remediar**: proporcionar información a los usuarios finales sobre cómo pueden remediar las infecciones de bots y/o ayudar activamente a los clientes empresariales a remediar los impactos de las redes de bots; y
- **Colaborar**: proporcionar información y experiencias aprendidas a otros PSI.

Soluciones emergentes

El ecosistema de Internet sigue mejorando su capacidad para mitigar los ataques de las redes de bots. Se están realizando esfuerzos para mejorar tanto las capacidades de detección como de mitigación.

Enfoques tecnológicos. Un gran número de programas maliciosos utiliza una técnica conocida como algoritmo de generación de dominios (DGA) para generar periódicamente un gran número de nombres de dominio que pueden ser utilizados como puntos de encuentro para sus servidores de C&C en un intento de ofuscar la verdadera infraestructura de la botnet. Actualmente, los investigadores de seguridad pueden trabajar en la ingeniería inversa del DGA utilizado por cada variante de malware. La ingeniería inversa puede ser un proceso largo, y a menudo es un enfoque ineficaz de tipo "whack-a-mole". Para solucionar este problema, la industria ha estado investigando cómo aplicar el aprendizaje automático para automatizar el proceso y trabajar en tiempo real como

[34] Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG), *ABCs for ISPs*, disponible en https://www.m3aawg.org/abcs-for- ISP-code (consultado el 20 de junio de 2017).

el malware registra nombres de dominio en un registro de Internet. Se están realizando esfuerzos para comercializar e integrar el aprendizaje automático para la detección de botnets en los productos de protección de la red.

Las redes de bots más recientes suelen utilizar el cifrado (por ejemplo, TLS35) para ocultar su canal de C&C. El proyecto Secure Sockets Layer SSL Blacklist (SSBL)36 ilustra que, aunque la red de bots utilice el cifrado, todavía es posible detectar la red de bots. Es posible identificar el tráfico de C&C del bot inspeccionando los certificados SSL maliciosos para generar una huella digital SHA-137 única para cada botnet utilizando la inspección profunda de paquetes (DPI). Se están realizando esfuerzos para comercializar este enfoque e integrar los métodos en los sistemas de protección de la red para permitir la toma de huellas digitales en tiempo real y la mitigación de las redes de bots.

Además, los investigadores están desarrollando el uso de tarpits a escala de red para frenar la propagación de las redes de bots. [38] Los investigadores están estudiando cómo convertir el espacio de direcciones IP no utilizadas en tarpits para botnets. [39] La idea básica es dirigir todo el tráfico entrante que se dirige a las direcciones IP no utilizadas al tarpit. El tarpit tiene un conjunto de reglas programadas sobre cómo responder y, por lo tanto, prolonga el tiempo que tarda una red de bots en abrirse camino hasta la cadena de muerte. [40] Al prolongar el tiempo, los objetivos del ataque tienen más tiempo para determinar qué medidas defensivas adicionales hay que poner en marcha para neutralizar el ataque, si es que hay alguna.

Además de los tarpits, los proveedores de redes han emprendido esfuerzos para determinar cómo aprovechar las características de las redes definidas por software (SDN) para ayudar a mitigar los ataques de las redes de bots. Las SDN proporcionan la capacidad de crear dinámicamente redes superpuestas. Cuando se combinan con otras técnicas y tecnologías de partición de la red, es posible crear dinámicamente carriles virtuales para los diferentes servicios basados en IP. Con este enfoque, los proveedores de IoT pueden trabajar con los proveedores de servicios de red para crear carriles virtuales de extremo a extremo desde el dispositivo IoT a través de la red hasta el servicio basado en la nube. Este proceso garantiza que un dispositivo IoT comprometido no pueda

---

[35E]. Rescorla y N. Modaugu, *Datagram Transport Layer Security Version 1.2*, IETF Tools (enero de 2012), disponible en https://tools.ietf.org/html/rfc6347 (consultado el 20 de junio de 2017).

[36] SSL Blacklist, *SSL Blacklist*, disponible en https://sslbl.abuse.ch/blacklist/ (consultado el 20 de junio de 2017).

[37] SHA-1 - Secure Hash Algorithm 1 es una función hash criptográfica que genera una clave hash de 20 bytes utilizada por muchas aplicaciones y protocolos de seguridad, incluyendo TLS y SSL, como parte del cifrado de datos.

[38] Labrea, *Tom Liston Talks about Labrea*, disponible en http://labrea.sourceforge.net/Intro-History.html (consultado el 17 de julio de 2017).

[39] Los tarpits son medidas defensivas contra los ataques en los que el servidor retrasa a propósito las conexiones entrantes para que el spam y el escaneo amplio sean menos efectivos.

[40] Eric Hutchins, Michael Cloppert y Rohan Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, CND Papers (21 de noviembre de 2010), disponible en http://papers.rohanamin.com/?p=15 (consultado el 7 de julio de 2017).

comunicarse con puntos finales no autorizados. En otras palabras, un dispositivo comprometido no podría ser utilizado en un ataque DDoS o enviar información a hosts no autorizados. La función Network Slicing de las redes 5G es un buen ejemplo de [ello41] , y se están investigando enfoques similares para las redes cableadas con SDN.

Iniciativas de colaboración. Se están llevando a cabo varias iniciativas dirigidas por la industria para mejorar el intercambio automático de información sobre ciberamenazas. La Ley de Intercambio de Información sobre Ciberseguridad (CISA), promulgada en 2015, y el posterior despliegue de la capacidad de Intercambio de Información Automatizada (AIS) del DHS están ayudando a facilitar las iniciativas de máquina a máquina (M2M).

Hay al menos otras dos iniciativas de intercambio automatizado de M2M que pueden ser útiles para combatir las redes de bots. Ambas tienen el objetivo común de garantizar que la información sobre ciberamenazas que se comparte sea "procesable" por el receptor. El paradigma en el pasado ha sido a menudo que las redes traten de construir una mejor protección en sus puntos de entrada a la red. Estas iniciativas comparten información con las redes vecinas para mitigar la amenaza lo más cerca posible del origen del tráfico malicioso.

El Grupo de Trabajo de Ingeniería de Internet (IETF) está desarrollando un protocolo denominado DDOS Open Threat Signaling (DOTS)[42] para el intercambio en tiempo real de telemetría relacionada con los DDoS entre los elementos de la red de mitigación de DDoS. El protocolo DOTS del IETF está trabajando para mejorar la cooperación entre las víctimas de ataques DDoS y las partes que pueden ayudar a mitigar dichos ataques. El protocolo apoyará las solicitudes de servicios de mitigación de DDoS y las actualizaciones de estado a través de los límites administrativos entre organizaciones (por ejemplo, de red a red).

Los miembros del grupo de interés especial en DDoS del Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG)43 están colaborando en un esfuerzo similar. El M3AAWG está desarrollando una interfaz de programa de aplicación (API), un almacén de datos e implementaciones de referencia de código abierto para que los proveedores de servicios de red compartan indicadores de amenazas DDoS con el fin de identificar las fuentes del tráfico de ataques DDoS, pero no para mitigar los ataques en tiempo real. El enfoque del M3AAWG permite a los proveedores de servicios de red compartir las direcciones IP de origen de los flujos IP entrantes que sus sistemas de detección de DDoS identifican de forma anónima con la red en la que el DDoS

---

[41] *Véase* 5G Americas, *Network Slicing for 5G Networks & Services,* disponible en http://www.5gamericas.org/files/3214/7975/0104/5G_Americas_Network_Slicing_11.21_Final.pdf (consultado el 7 de julio de 2017).
[42] IETF, *DDoS Open Threat Signaling (puntos)*, disponible en https://datatracker.ietf.org/wg/dots/about/ (consultado el 20 de junio de 2017). [43] M3AAWG, *M3AAWG publica nuevos documentos que explican la seguridad de las contraseñas, la autenticación multifactorial, el uso de la encriptación y las salvaguardias DDoS; anuncia la dirección y los presidentes de los comités*, comunicado de prensa (4 de abril de 2017), disponible en https://www.m3aawg.org/news/rel-leadership-papers-2017-04 (consultado el 20 de junio de 2017).

ataque originado. Esto permite a los operadores de red limpiar las fuentes del tráfico de ataques DDoS. Al compartir sólo la dirección IP de origen, este enfoque es compatible con la mayoría de las leyes mundiales de privacidad con respecto al intercambio de información identificable.

Retos y oportunidades

La ciberseguridad es una responsabilidad compartida. Reducir las amenazas de los bots, las redes de bots y sus ataques automatizados requiere la cooperación y la colaboración de todos los miembros del ecosistema de Internet. Esta sección identifica una serie de áreas en las que las amenazas presentadas por los bots y las redes de bots pueden reducirse con una mejor cooperación y colaboración de los miembros del ecosistema de Internet.

Retirada de botnets

Desafío - Ninguna técnica es más eficaz que las acciones policiales que conducen a la detención de los autores. Esta es la única solución que aborda la raíz del problema, y no sólo un síntoma. Por desgracia, la ejecución de un desmantelamiento de una red de bots requiere un importante análisis forense previo y una cuidadosa coordinación entre muchas partes interesadas, a menudo a través de las fronteras internacionales. Un factor que limita la velocidad global de los desmantelamientos de botnets es la falta de recursos de las fuerzas de seguridad. El otro reto es que la mayoría de las redes de bots son de naturaleza internacional, lo que requiere una cooperación entre países que requiere muchos recursos y tiempo.

Oportunidad - El aumento de los recursos de las fuerzas de seguridad y la racionalización de los procesos internacionales contribuirían al proceso general de desmantelamiento de las redes de bots.

Información sobre amenazas cibernéticas procesable

Reto - Los proveedores de servicios de red deben disponer de información precisa y procesable sobre ciberamenazas para poder neutralizar rápidamente las redes de bots. Para que la información sea procesable, el indicador de ciberamenazas tiene que estar correlacionado con un único punto final. Muchas de las fuentes de datos utilizadas y compartidas por las empresas son listas de reputación de IP a largo plazo de poco valor para los proveedores de servicios de red que operan redes con un gran conjunto de suscriptores que tienen direcciones IP asignadas dinámicamente con arrendamientos cortos. Esto significa que el indicador de ciberamenazas debe ser oportuno e incluir la dirección IP actual o la dirección IP y una marca de tiempo de la actividad maliciosa.

Lo mismo ocurre con las direcciones IP de los servidores de C&C de la botnet. Los servidores de C&C no suelen *tener* una dirección IP estática. A menudo, los servidores de C&C se encuentran en hosts compartidos donde una única dirección IP es compartida por varios hosts. Además, los servidores de C&C pueden tener un grupo de direcciones IP o hosts compartidos por los que rotan.

Los proveedores de servicios de red necesitan una indicación única, altamente fiable y a corto plazo de que una dirección IP ha generado tráfico malicioso o ha sido escaneada para mostrar los servicios vulnerables expuestos, así como los hosts comprometidos.

Oportunidades - Los expertos coinciden en que la información sobre ciberamenazas debe ser oportuna y específica para ser eficaz. Las iniciativas de intercambio de información cibernética del Grupo de Trabajo DOTS del IETF y el M3AAWG DDoS SIG son pasos en la dirección correcta. El AIS del DHS[44] también ofrece una oportunidad para mejorar y potenciar el intercambio oportuno y adaptado de indicadores de ciberamenazas para satisfacer las necesidades de los destinatarios.

Traducción de direcciones de red

Desafío - Los ISP alámbricos que operan redes IPv4 suelen proporcionar a un abonado residencial una única dirección IPv4 pública. El abonado residencial suele utilizar un router doméstico que incluye una función de traducción de direcciones de red (NAT), lo que le permite compartir su única dirección IPv4 pública con varios dispositivos en el hogar.

Cuando un ISP recibe información sobre un abonado residencial que envía tráfico malicioso, esa información, en el mejor de los casos, sólo puede contener la dirección IPv4 asignada al cliente y no la del punto final real detrás del router doméstico. El uso de la tecnología NAT dificulta al ISP la identificación del dispositivo específico en el hogar del abonado que está enviando tráfico malicioso.

Oportunidad - IPv6 elimina la necesidad de utilizar NAT para compartir direcciones IP, ya que cada dispositivo conectado a Internet puede tener una dirección IPv6 enrutable públicamente. Aunque no es una panacea, la eliminación de los routers NAT puede facilitar la identificación de los dispositivos finales que transmiten tráfico malicioso en determinadas circunstancias, y filtrar el tráfico sospechoso adecuadamente. A partir de junio

[44] DHS, *Automated Indicator Sharing (AIS)*, disponible en https://www.dhs.gov/ais (consultado el 20 de junio de 2017).

En 2017, la adopción de IPv6 por parte de los proveedores de redes fue de aproximadamente el 19% a nivel mundial,[45] y del 35% y en aumento dentro de Estados Unidos.

Tráfico fuera de la red

Desafíos - Al tratarse de redes globales ampliamente distribuidas, la mayoría de los bots y sus servidores de C&C están fuera de la red y del control administrativo del proveedor de servicios de red. De hecho, numerosos informes dejan claro que la abrumadora mayoría del tráfico de las redes de bots se origina fuera de los Estados Unidos. [46]

Además, en la mayoría de los casos, sólo una pequeña parte de los puntos finales de un proveedor de servicios de red puede estar infectada por una sola red de bots, y la cantidad de tráfico generado por la red de bots será minúscula. Esta pequeña cantidad de tráfico puede ser muy difícil de detectar, ya que no activará muchos de los umbrales de supervisión de la red que un proveedor de servicios de red tiene en su lugar.

Oportunidad - Para hacer frente a estos dos retos es necesaria la colaboración entre los proveedores de servicios de red, ya que una de las medidas más eficaces es filtrar el tráfico lo más cerca posible del dispositivo infectado con el bot. Cualquier acuerdo de tránsito o peering debe incluir un lenguaje que aborde la disponibilidad y la depuración del tráfico para permitir que los operadores de red soliciten al proveedor o proveedores anteriores que filtren el tráfico malicioso.

Notificaciones al usuario final

Desafío - Notificar y conseguir que los usuarios finales actúen sigue siendo un desafío. Los miembros del ecosistema de Internet pueden notificar al usuario final de múltiples maneras:[47]

- Correo electrónico;
- Llamada telefónica;
- Correo postal;

---

[45] Google, *IPv6 Adoption* (18 de junio de 2017), disponible en https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6- adoption&tab=per-country-ipv6-adoption (consultado el 20 de junio de 2017).
[46] Incapsula.com, *Global DDoS Threat Landscape Q4 2016* (Invierno 2017), disponible en https://www.incapsula.com/ddos-report/ddos- report-q4-2016.html (consultado el 20 de junio de 2017).
[47] Michael Glenn, *Malware Notification and Remediation Tools and Techniques*, presentación de CenturyLink en el taller del NIST: Technical Aspects of Botnet (30 de mayo de 2012), disponible en https://www.nist.gov/sites/default/files/documents/itl/csd/centurylink_malware_notification_and_remediation.pdf (consultado el 20 de junio de 2017).

- Mensaje de texto;
- Notificación del navegador web;
- Jardín amurallado; y
- Otros métodos. [48]

Un estudio encargado por el M3AAWG para determinar la eficacia de varios métodos de notificación y reparación mostró que los dos métodos más eficaces son una llamada telefónica al usuario del dispositivo y el correo postal. [49] El creciente uso de dispositivos IoT en los hogares presenta nuevos retos a la hora de notificar a los usuarios finales. Los dispositivos IoT suelen tener interfaces de usuario limitadas, lo que anula varios de los métodos de notificación (navegador web, walled garden, etc.). Esto se ve agravado por el hecho de que un ISP sólo puede notificar a un usuario final que "un dispositivo" en su casa está infectado, y no puede identificar el dispositivo corrupto específico.

Oportunidades - Existen varias medidas para mejorar la identificación de los dispositivos en el futuro. Unos dispositivos IoT mejor diseñados que se adhieran a los estándares de la industria, como los que está desarrollando la Open Connectivity Foundation (OCF)[50] , son una vía para mejorar la seguridad. Y, como se ha señalado anteriormente, la compatibilidad del operador de red con IPv6 ayudará tanto a la identificación del dispositivo infectado como a la notificación al usuario del dispositivo.

DNS de flujo rápido

Reto - El uso de fast flux51 por parte de malware y botnets para ocultar su infraestructura sigue creciendo. El fast flux es una técnica de DNS en la que numerosas direcciones IP asociadas a un mismo nombre de dominio entran y salen con una frecuencia extremadamente alta. Fast flux oculta eficazmente los ordenadores o servidores que realizan los ataques maliciosos para que no sean detectados. El fast flux hace que cortar el contacto de los bots con los servidores de C&C sea difícil o imposible sólo con el filtrado de direcciones IP.

Oportunidad - En 2008, el Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN publicó un aviso de seguridad en el que se hacían una serie de recomendaciones de mitigación para abordar el DNS de flujo rápido

---

[48] Otros métodos pueden ser un mensaje en las redes sociales, una alerta en el televisor a través del descodificador, un mensaje en el buzón de voz del depósito directo, etc.
[49] Investigadores de Georgia Tech, *DNS Changer Remediation Study*, Presentation to M3AAWG 27th General Meeting, San Francisco, CA (Feb. 19, 2013), disponible en https://www.m3aawg.org/sites/default/files/document/GeorgiaTech_DNSChanger_Study-2013-02-19. pdf (consultado el 20 de junio de 2017).
[50] *Véase* Open Connectivity Foundation, disponible en https://openconnectivity.org/ (consultado el 20 de junio de 2017).
[51] Comité Asesor de Seguridad y Estabilidad de ICANN (SSAC), *SAC 025 SSAC Advisory on Fast Flux Hosting and DNS* (Mar. 2008), disponible en https://www.icann.org/en/system/files/files/sac-025-en.pdf (consultado el 20 de junio de 2017).

técnicas. Entre sus conclusiones y recomendaciones, el SSAC animó a ICANN, a los registros y a los registradores a tener en cuenta las prácticas de mitigación del flujo rápido en el asesoramiento.

Desde entonces, los avances en el aprendizaje automático se han aplicado a la detección de botnets mediante técnicas de DNS de flujo rápido. Los avances en la aplicación del aprendizaje automático para detectar redes de bots que realizan cambios en las entradas DNS permiten la automatización y la integración en los sistemas de detección de redes de bots.

Dispositivos IoT inseguros

Reto - Como se ha comentado a lo largo de este documento, la creciente base instalada de dispositivos IoT está haciendo que dichos dispositivos sean objetivos atractivos para que los ciberdelincuentes los infecten con código bot. Un buen ejemplo es el reciente ataque de la red de bots Mirai, en el que se infectaron cámaras de seguridad IoT no seguras y conectadas a Internet para generar un ataque masivo de DDoS. Este no es un fenómeno nuevo; el problema existe desde hace años, ya que durante años, muchos routers domésticos de consumo se enviaron con vulnerabilidades conocidas que han sido explotadas para generar ataques de amplificación de DNS a gran escala.

Los tipos de vulnerabilidades conocidas52 que se encuentran en muchos dispositivos IoT del mercado actual incluyen:

- Envío de dispositivos IoT con software desactualizado que contiene vulnerabilidades conocidas y que carece de la capacidad para una actualización automática del software;
- Protección sólo mediante nombres de usuario y contraseñas predeterminados de fábrica o codificados;
- Comunicaciones no autentificadas;
- Comunicaciones no encriptadas; y
- Falta de autenticación y autorización mutua.

Los dispositivos IoT inseguros presentan un desafío único, ya que una vez que se ven comprometidos, a menudo es imposible que el usuario final detecte que han sido comprometidos y, como se señaló anteriormente, es difícil que un proveedor de servicios de red notifique al usuario final que su dispositivo ha sido comprometido. Incluso después de que el usuario final sea consciente del compromiso, a menudo es imposible

52Grupo de Asesoramiento Técnico de Internet de Banda Ancha (BITAG), *Internet of Things Security and Privacy Recommendations* (Nov. 2016), disponible en http://bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf (consultado el 20 de junio de 2017).

remediar el problema debido a la falta de una actualización de software y/o a la falta de actualizaciones de software automatizadas.

Oportunidad - Los dispositivos IoT pueden estar mejor protegidos mediante el uso de aislamiento de red/ruta. [53] Las técnicas de aislamiento de red/ruta (VPNs, VLANs, enrutamiento basado en políticas, corte de red, etc.) pueden utilizarse para crear rutas lógicas de tráfico independientes. Estas rutas lógicas de tráfico independientes garantizan que el tráfico del IoT sólo pueda llegar a los puntos finales designados. Esto ayuda a mitigar los impactos de cualquier tráfico malicioso que un dispositivo IoT comprometido pueda enviar.

Con los avances en la virtualización de funciones de red (NFV) y las SDN, existen oportunidades para que los fabricantes de IoT diseñen dispositivos que utilicen técnicas de aislamiento de red/ruta como parte de su servicio. Además, existen oportunidades para que los proveedores de servicios de red ofrezcan el aislamiento de red/ruta como un servicio a los proveedores de IoT o a los usuarios finales para sus dispositivos de IoT.

Ataques de amplificación

Reto - Un ataque de amplificación es un tipo de ataque DDoS que se aprovecha del hecho de que una pequeña consulta, como una consulta DNS, puede generar una respuesta mucho mayor. Cuando se combina con la suplantación de la dirección de origen, un atacante puede dirigir un gran volumen de tráfico de red a un sistema objetivo. La naturaleza asimétrica de los ataques de amplificación los convierte en la opción preferida para los ataques DDoS. Los ataques de amplificación suelen aprovechar los protocolos basados en UDP, como el protocolo DNS, el protocolo de tiempo de red (NTP), el generador de caracteres (CharGEN) y la cita del día (QOTD).
Aproximadamente 15 protocolos de Internet son susceptibles de sufrir ataques de amplificación. [54] Los ingenieros de Internet desarrollaron una extensión del protocolo DNS, llamada DNS Security (DNSSEC) para solucionar la vulnerabilidad del DNS al envenenamiento de la caché del DNS. Desafortunadamente, un efecto secundario de esta solución es que la extensión de seguridad del DNS hace que las respuestas del DNS sean mucho más grandes y ayuda a amplificar aún más el ataque.

La implementación de la validación de la dirección de origen (SAV)[55] , tal y como se recomienda en el IETF BCP 38/84, evita los ataques de amplificación con direcciones de origen falsas. Aunque la mayoría de los grandes

---

[53] Cisco, *Network Virtualization--Path Isolation Design Guide* (22 de julio de 2008), disponible en http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html (consultado el 20 de junio de 2017). 54Equipo de Preparación para Emergencias Informáticas de Estados Unidos (US-CERT), *UDP-Based Amplification Attacks*, Alert (TA14-017A) (4 de noviembre de 2016), disponible en https://www.us-cert.gov/ncas/alerts/TA14-017A (consultado el 20 de junio de 2017).
[55] El SAV es una práctica recomendada por los ISP desde hace mucho tiempo (véase el IETF 2267 publicado en 1998), pero debido a la dificultad de aplicar el SAV en algunas situaciones comerciales, puede que no se aplique completamente en las redes de los ISP.

proveedores de servicios de red[56] han implementado la validación de la dirección de origen, aproximadamente el 30% del espacio total de direcciones IP sigue siendo falsificable. [57]

Oportunidad - El uso del filtrado de IP o de la validación de la dirección de origen (SAV), tal y como se indica en las mejores prácticas comunes (BCP) 38 y 84 del IETF para las direcciones IP falsas, es una técnica probada para mitigar los ataques de amplificación DDoS que utilizan direcciones de origen falsas.

Las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS)[58] son un esfuerzo liderado por la industria para codificar un conjunto de valores compartidos por los operadores de redes en un conjunto de definiciones y comportamientos ideales. Las MANRS recomiendan la aplicación de filtros anti-spoofing para evitar que entren o salgan de la red paquetes con direcciones IP de origen incorrectas. Hasta la fecha, más de 45 operadores de red participan en MANRS. Existe la oportunidad de conseguir que el espacio de direcciones falsificables sea casi nulo si todos los operadores de red participan en MANRS.

Gestión de la red coordinada de red a red

Desafío - Aunque la gestión de la red puede parecer sencilla y deseable, no está exenta de desafíos, sobre todo teniendo en cuenta el impacto negativo en los usuarios finales de Internet. Lo ideal sería que las mitigaciones de las redes de bots fueran rápidas y estuvieran dirigidas al origen del ataque. Los avances en la arquitectura de las redes mediante SDN y el uso de indicadores de ciberamenazas compartidos de forma automatizada por M2M empiezan a hacer técnicamente viable que los operadores de redes automaticen la coordinación de sus mitigaciones de botnets y reduzcan el tiempo de respuesta cuando se detecta un bot malicioso en una red o cuando un botnet inicia un ataque. Pero hay desafíos, que van desde lo técnico a lo contractual, y cuestiones de política.

Los desafíos técnicos incluyen tanto la detección como la mitigación. Sin una fuente de verdad básica para saber qué es y qué no es tráfico de botnets, dado que el tráfico de botnets suele estar diseñado para parecerse al tráfico normal de Internet, existe la posibilidad de que se produzcan falsos positivos. Incluso con una fuente de verdad, los métodos de mitigación de las redes de bots variarán de una red a otra debido a las diferencias inherentes a

---

[56] MANRS, *Participants* (6 de marzo de 2015), disponible en https://www.routingmanifesto.org/participants/ (consultado el 20 de junio de 2017). [57] Center for Applied Internet Data Analysis, *State of IP Spoofing*, disponible en https://spoofer.caida.org/summary.php (consultado el 20 de junio de 2017).
[58] MANRS, *Documento de Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS)* (8 de septiembre de 2016), disponible en http://www.routingmanifesto.org/manrs/ (consultado el 20 de junio de 2017).

cómo se diseñan y construyen las redes, así como las diferencias en los acuerdos de nivel de servicio entre los proveedores de servicios de red y sus clientes.

Mitigar a ciegas las redes de bots mediante el uso de la automatización está plagado de riesgos. Hay muchos casos en los que un servidor de mando y control no es propiedad o está completamente bajo el control del operador del bot, como por ejemplo 1) servidores DNS compartidos, 2) IPs compartidas y 3) sitios web públicos.[59] La aplicación ciega de un método de mitigación de botnets, como el filtrado de la dirección IP, impediría el acceso a todos los servicios que comparten el recurso (por ejemplo, DNS, servidor compartido o servicio). El reto no se limita a los recursos compartidos. Sin un conocimiento completo del acuerdo de nivel de servicio vigente entre el proveedor de servicios de red y el cliente, un servicio de red no puede filtrar ciegamente el tráfico hacia ese punto final.

Además, en el sector de las telecomunicaciones/ISP hay una tendencia emergente hacia la adopción de la SDN, que aún está en su fase inicial, pero que en general describe la automatización de la gestión y la orquestación de los activos y servicios de red. Por lo general, esto incluye el acoplamiento de marcos de big data que aprovechan el análisis avanzado y el aprendizaje automático para servir como bucles de retroalimentación para estas redes impulsadas por SDN para predecir, recomendar y prescribir en un esfuerzo por mejorar la capacidad de respuesta y la resistencia de sus activos y servicios. Tales implementaciones varían ampliamente en términos de capacidad y madurez entre los proveedores, y en la mayoría de los casos reflejan una propiedad intelectual altamente protegida que proporciona una experiencia competitiva única y
ofertas. No obstante, este ecosistema podría utilizarse como estrategia de mitigación de ataques. El despliegue de la SDN y de estas herramientas va mucho más allá de las fases conceptuales; son la complejidad y el coste de la implantación global en redes muy heterogéneas los que se erigen como obstáculos para la rapidez de los proveedores a la hora de implantarlas.

Oportunidad - Una mejor colaboración y coordinación puede reducir el tiempo de respuesta a las ciberamenazas. Como se ha mencionado anteriormente, la industria está desarrollando soluciones como el IETF DOTS, el piloto de intercambio de información del M3AAWG DDoS SIG y un piloto de intercambio de información dirigido por la CTIA que reducirá el tiempo de respuesta al compartir información sobre ciberamenazas "procesable". Además, a medida que las plataformas de intercambio de información sobre amenazas maduren en sus capacidades, esto ayudará a reducir el tiempo de respuesta de los operadores de red.

[59] Los sitios web públicos incluyen sitios como Twitter, Amazon AWS, Google Cloud y Rapidshare.

La clave para el éxito de la gestión coordinada de la red contra los botnets es la colaboración y la comunicación estrecha y de confianza entre las partes interesadas.

Recomendaciones del sector

Este documento expone algunos de los problemas que presentan los bots y las redes de bots, así como los retos y las oportunidades a los que se enfrentan los propietarios y operadores de redes de banda ancha. La siguiente sección se centra en las recomendaciones preliminares que pueden ser accionables no sólo por los proveedores de servicios de red sino por todo el ecosistema de Internet para ayudar a reducir las amenazas de los botnets utilizando la tecnología existente. Las recomendaciones preliminares aquí son desde la perspectiva del CSCC. Es necesario debatir las mejores prácticas y capacidades para todos los segmentos del ecosistema, incluidos los desarrolladores de software junto con los proveedores de infraestructuras de nube, alojamiento y aplicaciones.

Mitigación de ataques

- **Fomentar la migración continua a todo el IPv6.**

  El amplio uso de IPv6 permitirá que los dispositivos tengan una dirección única y puede facilitar la localización del origen del tráfico malicioso en determinadas circunstancias.

- **Garantizar que la información sobre ciberamenazas que se comparte es procesable y está adaptada a las necesidades de los destinatarios.**

  La información sobre ciberamenazas que se comparte entre las partes interesadas en Internet debe ser procesable por los destinatarios. Los participantes en el grupo de intercambio de información deben adaptar la información que comparten con sus compañeros para que sea procesable.

- **Incluir disposiciones prenegociadas para el filtrado del tráfico en los acuerdos de tránsito y de interconexión.**

  Los operadores de servicios de red de todos los tamaños (proveedores de servicios de Internet, empresas, gobiernos, instituciones educativas, etc.) y los usuarios finales deben asegurarse de que tienen disposiciones establecidas con sus

los proveedores de tránsito de Internet y las redes de interconexión para proporcionar el filtrado y la depuración del tráfico malicioso en sentido ascendente.

- **Agilizar el proceso de desmantelamiento de redes de bots por parte de las fuerzas de seguridad.**

  Las fuerzas del orden pueden desempeñar un papel fundamental en la neutralización de las redes de bots. Es necesario realizar esfuerzos para agilizar el proceso de aplicación de la ley para aumentar la velocidad y la eficacia de los desmantelamientos de botnets por parte de las fuerzas del orden.

- **Animar a ICANN, a los registros y a los registradores a que adopten las técnicas de mitigación de fast flux del SAC 025 SSAC Advisory on Fast Flux Hosting and DNS.**

  El ecosistema de Internet debería animar a ICANN, a los registros y a los registradores a que consideren y adopten las técnicas de mitigación de flujo rápido del asesoramiento del SSAC.

- **Adaptar y aplicar el aprendizaje automático a la detección de botnets.**

  El ecosistema de Internet debería dejar de invertir manualmente los algoritmos de generación de dominios de botnets y empezar a aplicar el aprendizaje automático para automatizar la detección en tiempo real de botnets que utilizan flujo rápido, cifrado y otras técnicas para enmascarar su infraestructura.

Prevención de puntos finales

- **Asegúrese de que todos los puntos finales, incluidos los dispositivos IoT, cumplen las normas de seguridad desarrolladas por el sector.**

  Se están llevando a cabo múltiples esfuerzos liderados por la industria para desarrollar estándares de seguridad para los dispositivos IoT. Los fabricantes de dispositivos IoT y los proveedores de servicios IoT deben trabajar para garantizar que todos los dispositivos IoT se adhieran a las normas de seguridad de sus respectivos sectores y a las mejores prácticas de seguridad IoT.

- **Asegúrese de que los puntos finales ejecutan software actualizado.**

  Como dice el refrán "más vale prevenir que curar". Esto se aplica también a los puntos finales de los consumidores/clientes. Garantizar que todos los puntos finales (ordenadores de sobremesa, móviles, IoT, etc.) ejecuten software actualizado con los últimos parches y actualizaciones de seguridad.

ayudará enormemente a reducir el número de puntos finales infectados y comprometidos en Internet.

- **Los dispositivos IoT deben utilizar técnicas de aislamiento de la red y/o de filtrado basado en la red para cualquier comunicación con los servicios basados en la nube.**

  El aislamiento de la red y/o el filtrado basado en la red son técnicas probadas para reducir la capacidad de un punto final de Internet no autorizado para hacer daño. [60] Los fabricantes de dispositivos IoT y los proveedores de servicios IoT deberían diseñar sus productos y servicios para hacer uso de estas técnicas.

Conclusión:

La ciberseguridad es una responsabilidad compartida. Proteger Internet de las amenazas de las redes de bots requiere la colaboración y cooperación de todos los miembros del ecosistema de Internet, tanto a nivel nacional como internacional. Las recomendaciones preliminares de este documento representan sólo algunas de las muchas maneras en que las amenazas de las botnets y su capacidad de daño pueden reducirse mediante un amplio compromiso de las partes interesadas.

Sobre los autores

Matt Tooley es el Vicepresidente de Tecnología de Banda Ancha de la NCTA - Asociación de Internet y Televisión. Es miembro del Comité Ejecutivo del Consejo de Coordinación del Sector de las Comunicaciones. Tooley tiene más de 30 años de experiencia en el sector de la banda ancha en el desarrollo y despliegue de tecnología de banda ancha para proveedores de servicios de Internet.

Este documento incluye contribuciones clave de AT&T, CenturyLink y Cox Communications.

[60] BITAG, *Internet of Things (IoT) Security and Privacy Recommendations* (noviembre de 2016) en la sección 6 (en la que se analiza "A possible role for in- home network technology"), disponible en http://bitag.org/documents/BITAG_Report_-_Internet_de_las_Cosas_(IoT)_Seguridad_y_Privacidad_Recomendaciones.pdf (consultado el 20 de junio de 2017).

Apéndice A - Informes sobre ciberamenazas

Los 10 peores países en cuanto a redes de bots		
Rango	**País**	**Número de bots**
1	China	1,375,637
2	India	958,814
3	Federación de Rusia	569,463
4	Brasil	429,942
5	Vietnam	380,639
6	Irán, República Islámica de	242,909
7	Argentina	177,701
8	Tailandia	173,027
9	México	145,516
10	C?*	141,684

Fuente: Spamhaus a 29 de junio de 2017. https://www.spamhaus.org/statistics/botnet-cc/

** Spamhaus informa que el décimo país de esta lista es "C?".*

Los 10 países que más tráfico de botnets atacan		
Rango	**País**	**Porcentaje de tráfico de ataque**
1	China	50.8%
2	Corea del Sur	10.8%
3	Estados Unidos	7.2%
4	Egipto	3.2%
5	Hong Kong	3.2%
6	Vietnam	2.6%
7	Taiwán	2.4%
8	Tailandia	1.6%
9	Reino Unido	1.5%
10	Turquía	1.4%

Fuente: Incapsula Global DDoS Threat Landscape Q1 2017. https://www.incapsula.com/ddos- report/ddos-report-q1-2017.html

Principales países por % de direcciones IP de países que participan en ataques DDoS, primer trimestre de 201661

Q1 2016		Q2 2016		Q3 2016		Q4 2016	
País	% de países Direcciones IP	País	% de países Direcciones IP	País	% de países Direcciones IP	País	% de países Direcciones IP
	IPs de origen		IPs de origen		IPs de origen		IPs de origen
Turquía	0.282%	Vietnam	0.130%	REINO UNIDO	0.036%	Rusia	0.078%
	43,400		20,244		44,460		33,211
Brasil	0.075%	China	0.093%	Brasil	0.025%	REINO UNIDO	0.059%
	36,472		306,627		81,276		72,949
China	0.035%	Taiwán	0.081%	China	0.025%	Alemania	0.042%
	115,478		28,546		81,276		49,408
Corea del Sur	0.028%	Canadá	0.026%	Francia	0.025%	China	0.014%
	31,692		20,601		23,980		46,783
ESTADOS UNIDOS.	0.005%	ESTADOS UNIDOS.	0.006%	ESTADOS UNIDOS.	0.004%	ESTADOS UNIDOS.	0.012%
	72,598		95,004		59,350		180,652

Fuentes:

Informe de Akamai sobre el estado de la seguridad en Internet del cuarto trimestre de 2016.
https://www.akamai.com/us/en/multimedia/documents/state-of-the- internet/q4-2016-state-of-the-internet-security-report.pdf

Colaboradores de Wikipedia, "Lista de países por asignación de direcciones IPv4", *Wikipedia, La enciclopedia libre*,https://en.wikipedia.org/w/index.php?title=List_of_countries_by_IPv4_address_allocation&oldid=776891748 (consultado el 17 de julio de 2017).

[61] El número de IPs de origen que participan en ataques DDoS procede del informe Akamai State of Internet Security Report Q4 2016. Los datos se han normalizado según el porcentaje de direcciones IPv4 asignadas a un país a partir de los datos de la IANA en el momento de redactar este documento. Los porcentajes pueden variar un poco desde el momento del informe de Akamai.

Apéndice B - Amenazas de las redes de bots

Fraude por clic

Las páginas web suelen ser pagadas por los anunciantes. Los anunciantes pagan por el número de "clics" o visitas al sitio web del anunciante. Si un sitio web o un agente publicitario es capaz de generar la percepción de que mucha gente visita un anuncio, obliga al anunciante a pagar por cada una de esas visitas. Una forma de generar muchos clics es ordenar a una red de bots que genere esas visitas.

Correo electrónico de spam, phishing o malware

Las redes de bots se utilizan a menudo para originar correo electrónico masivo no solicitado, que también puede incluir la distribución de malware de varios tipos, como ransomware, enlaces a sitios de phishing y malware asociado a bots. Las redes de bots también pueden utilizarse para enviar propaganda comercial no solicitada más mundana.

Puerta de red no autorizada

Los bots dentro de los límites de una red protegida, como una red empresarial, pueden convertirse en puertas de enlace no autorizadas dentro de los límites protegidos, y pueden utilizarse para obtener acceso a otros recursos (datos u ordenadores) dentro de los límites protegidos (también conocido como movimiento lateral).

Robo de datos

Los bots pueden robar datos de los dispositivos infectados a través de medios como la monitorización de la red, el registro de claves o el raspado de datos de la memoria o el disco. Esto se consigue con frecuencia porque muchos miembros de los bots se sitúan dentro de las redes privadas y empresariales junto a los activos que contienen los datos valiosos. Una gran cantidad de robos de datos se realiza hoy en día mediante ataques de "Spear Phishing "[62] , en los que se envían correos electrónicos de apariencia válida a una persona de una empresa y ese correo se utiliza para robar propiedad intelectual o información bancaria, o para alojar malware. Un ataque típico puede consistir en que el "malhechor" envíe un correo electrónico a un asistente administrativo o a otro empleado de nivel inferior que parezca provenir de un alto ejecutivo, en el que el "ejecutivo" pide al destinatario del correo electrónico que restablezca una contraseña porque hoy hay que pagar una "factura". El destinatario restablecerá la

---

[62] Federal Bureau of Investigation (FBI), *Spear Phishers* (1 de abril de 2009), disponible en https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109 (consultado el 17 de julio de 2017).

contraseña utilizando enlaces ofuscados que contienen malware en el correo electrónico. Esto permite que comience la infección y que la instalación del software APT (Advanced Persistent Threat) realice actividades ilegales.

Distribución de contenidos ilícitos

Los bots se conectan a veces a las redes de intercambio de archivos peer-to-peer para ayudar a almacenar y distribuir contenidos ilegales.

Adquisición de contraseñas por fuerza bruta

Las redes de bots se utilizan para adivinar contraseñas por fuerza bruta. Uno de los métodos utiliza intentos de adivinación de contraseñas a alta velocidad utilizando un algoritmo de contraseñas aleatorias, un diccionario de contraseñas o una lista de contraseñas predefinidas. En primer lugar, la fuerza bruta puede ser utilizada por un miembro individual del bot como método de reclutamiento para infectar otros dispositivos mediante el escaneo de cualquier activo con un puerto abierto expuesto conocido y luego implementar uno de los métodos de fuerza bruta explicados para "adivinar" la contraseña. En segundo lugar, puede ser utilizado por un bot o una red de bots para forzar las credenciales de inicio de sesión de un objetivo previsto para obtener acceso a los privilegios o datos que la credencial proporciona.

Procesamiento Robo (por ejemplo, minería de Bitcoin)

Debido al número de miembros de bots que se suelen ver en las redes de bots, y al aumento del precio de las criptomonedas (por *ejemplo,* Bitcoin), las redes de bots se utilizan con mucha frecuencia para "minar" monedas. El proceso de minería de Bitcoins requiere la resolución de ecuaciones matemáticas muy complejas que, una vez resueltas, otorgan al minero un número determinado de monedas. Para tener éxito, un minero necesita una enorme cantidad de potencia de cálculo para resolver estas ecuaciones en el menor tiempo posible. Aquí es donde una red de bots puede ser extremadamente útil. Aprovechando la potencia de cálculo de un gran número de bots y "ordenando" a esos bots que actúen como mineros, el propietario de la red de bots puede utilizar el procesamiento combinado de muchos bots para hacer que la minería de Bitcoin sea muy lucrativa.

Las redes de bots también se han utilizado para aprovechar la potencia informática de los dispositivos infectados con el fin de realizar la minería de Bitcoin u otras actividades en beneficio de los actores maliciosos que dirigen la red de bots y no de los propietarios legítimos de los recursos informáticos.

Glosario

AIS - Automated Indicator Sharing, El Departamento de Seguridad Nacional (DHS) opera un servicio gratuito para el intercambio de indicadores de ciberamenazas.

Bot - Programa que se instala en un sistema para que éste realice automáticamente (o semiautomáticamente) una tarea o conjunto de tareas, normalmente bajo el mando y control de un administrador remoto (también conocido como bot master o bot herder).

Botnet - Red de dispositivos informáticos de usuario final conectados a Internet e infectados con malware bot, que son controlados remotamente por terceros con fines nefastos.

Mando y Control (C&C) - Un ordenador remoto utilizado para coordinar las acciones de los bots.

CTI - Indicador de Ciber Amenaza es la información necesaria para describir o identificar un atributo de una amenaza de ciberseguridad.

DDoS - El ataque de denegación de servicio distribuido es un intento de hacer que un servicio en línea no esté disponible abrumándolo con tráfico de múltiples fuentes.

DNS - El Sistema de Nombres de Dominio es el sistema de nomenclatura jerárquica descentralizada para los recursos conectados a Internet.

Tortura de agua DNS - Un tipo de ataque en el que muchos puntos finales envían consultas para el dominio de una víctima con una cadena aleatoria añadida al dominio que abruma al servidor DNS autoritario de la víctima y hace que el dominio de la víctima sea inaccesible.

DOTS - La señalización abierta de amenazas DDoS es un método por el cual un dispositivo o aplicación que participa en la mitigación de DDoS puede señalar información relacionada con el manejo de la amenaza actual a otros dispositivos o aplicaciones.

ICANN - Internet Corporation for Assigned Names and Numbers es la organización sin ánimo de lucro responsable de coordinar el mantenimiento y los procedimientos del espacio de nombres de Internet.

IRC - Internet Relay Chat es un protocolo de Internet que facilita la comunicación en texto utilizando una arquitectura cliente/servidor.

IoT - Internet of Things (Internet de los objetos) es el término general que hace referencia al desarrollo tecnológico en el que un número cada vez mayor de dispositivos están conectados entre sí y/o a Internet.

IPv4 - El Protocolo de Internet versión 4 es la cuarta versión del Protocolo de Internet (IP). El IPv4 es uno de los protocolos principales y sigue dirigiendo la mayor parte del tráfico de Internet en la actualidad.

IPv6 - La versión 6 del Protocolo de Internet es la sexta versión del Protocolo de Internet (IP). IPv6 es la versión más reciente y se desarrolló para hacer frente al problema previsto del agotamiento de las direcciones IPv4. IPv6 pretende sustituir a IPv4.

Kill Chain - Idea propuesta por Lockheed Martin para describir las fases de un ciberataque dirigido:
1) reconocimiento, 2) armamento, 3) entrega, 4) explotación, 5) instalación, 6) mando y control, y 7) acciones.

NAT - La traducción de direcciones de red es un método para reasignar un espacio de direcciones IP a otro modificando la dirección en las cabeceras de los paquetes IP para permitir que varios puntos finales compartan una dirección mientras transitan por un router de red.

Proveedor de servicios de **red -** Un proveedor u operador de servicios de red es cualquier empresa que opera una red que tiene un número de sistema autónomo (ASN) asignado.

Peering - El peering es la interconexión voluntaria de dos redes separadas con el fin de intercambiar tráfico entre los usuarios de cada red.

Peer-to-Peer (P2P) - Tradicionalmente, los clientes de los botnets se comunican con un servidor de C&C para recibir órdenes. Las redes de bots P2P funcionan sin un servidor de C&C y cada bot es a la vez un cliente y un servidor.

Redes definidas por software (SDN): enfoque de las redes informáticas que permite el control programático del comportamiento de la red mediante interfaces abiertas y la disociación del plano de reenvío de paquetes del plano de control para permitir el uso de servidores estándar y conmutadores Ethernet para proporcionar la función de enrutamiento en lugar de enrutadores especializados.

SSAC - El Comité Asesor de Seguridad y Estabilidad asesora a la comunidad de ICANN y a la Junta Directiva en asuntos relacionados con la seguridad e integridad de los sistemas de asignación de nombres y direcciones de Internet.

Tarpit - Un tarpit es un ordenador que retrasa a propósito las conexiones entrantes. Es una medida defensiva para hacer más lento el spam y el escaneo de la red. Es análogo a un pozo de alquitrán en el que los animales pueden empantanarse y hundirse lentamente bajo la superficie.

Tránsito **- El tránsito de Internet es** el servicio que permite que el tráfico de red "transite" por una red para llegar a otra. Los pequeños operadores de red y las empresas compran el tránsito de Internet para acceder a la red.