Botnets

Informe de Políticas de la Internet Society

Las botnets son un desafío complejo y en constante evolución que afecta la confianza del usuario y la seguridad en Internet. La lucha contra las botnets requiere colaboración transfronteriza y multidisciplinaria, enfoques técnicos innovadores y el despliegue generalizado de medidas de mitigación que respeten los principios fundamentales de Internet.

Introducción

Una botnet consiste en una colección o grupo de computadoras de usuarios conectadas a Internet (bots) infectadas con programas malignos (malware) que permite a un operador (operador o pastor de bots) controlar remotamente las computadoras a través de un servidor de comando y control (C&C) para realizar tareas automatizadas; como por ejemplo robar información o lanzar ataques contra otras computadoras. El malware tipo botnet está diseñado para permitir a sus operadores controlar las computadoras de muchos usuarios a la vez. Esto permite a los operadores de botnets utilizar los recursos informáticos y el ancho de banda de múltiples redes diferentes para actividades maliciosas.

Históricamente, las botnets se han utilizado principalmente para originar y propagar mensajes de correo no deseado (spam). Se pueden utilizar para muchos propósitos maliciosos, entre ellos: robar datos personales y contraseñas; atacar redes públicas y privadas; aprovecharse de las computadoras y el acceso a Internet de los usuarios; y llevar a cabo ataques distribuidos de denegación de servicio (DDoS).[1] En síntesis, las botnets constituyen un problema complejo y en permanente evolución que amenaza la confianza de los usuarios en Internet.

Son varias las técnicas que se utilizan para infectar computadoras de modo que se conviertan en bots, entre ellas: tentar a los usuarios para que descarguen malware; explotar vulnerabilidades de los navegadores de Internet; y engañar a los usuarios para que descarguen el malware cuando, por ejemplo, abren un archivo infectado adjunto a un mensaje de correo electrónico. A menudo un malware tipo botnet está diseñado para ejecutarse en segundo plano, de modo que los usuarios no se dan cuenta de que sus sistemas están infectados.

Aunque las botnets representan amenazas para los usuarios de Internet y son difíciles de eliminar, se pueden tomar medidas para reducir su impacto y riesgos asociados.

Consideraciones clave

Las botnets imponen costos económicos y sociales a los usuarios afectados, a los proveedores de servicios, a los operadores de red y a la sociedad en su conjunto. Sin esfuerzos eficaces para mitigar tales costos, las botnets conllevan el potencial podrían de reducir los beneficios económicos y sociales globales

[1] https://en.wikipedia.org/wiki/Denial-of-service_attack

que se derivan de Internet. Se deben considerar una serie de cuestiones ante el problema de las botnets, entre ellas las siguientes:

- **Dispersión geográfica.** Las botnets pueden estar distribuidas sobre áreas geográficas y distancias muy extensas; además, con hackers y computadoras infectadas operando en diferentes países y ubicaciones. Lo mismo aplica a los servidores C&C. Como tales, las botnets son transnacionales y requieren de colaboración para su detección, mitigación y la aplicación de la ley que aplique.
- **Impacto sobre los derechos de los usuarios.** Las estrategias de lucha contra las botnets debe considerar el impacto sobre los derechos fundamentales de los usuarios y sus expectativas. Las estrategias de mitigación de botnets excesivamente amplias —por ejemplo, bloquear todo el tráfico de una red infectada— podrían afectar que usuarios inocentes accedan a Internet y ejerzan sus derechos, entre ellos la libertad de expresión y opinión. Además, algunos de los métodos utilizados para detectar y rastrear botnets, como por ejemplo, la recolección indiscriminada del tráfico de red, podrían violar la privacidad de usuarios legítimos de Internet.
- **Impacto sobre el uso de la tecnología y la innovación.** Algunas de las estrategias técnicas y legales de mitigación, como por ejemplo, la restricción del acceso a redes presuntamente infectadas, pueden tener consecuencias negativas en el carácter abierto , el potencial de innovación y el alcance global del Internet. Además, es menos probable que estrategias diseñadas específicamente para una determinada tecnología aborden el problema global de las botnets, ya que sus creadores podrían cambiar de táctica para evitar nuevos obstáculos.

Desafíos

Una serie de factores contribuyen al desafío continuo de la lucha contra las botnets, entre ellos:

- Las estrategias, tecnologías y técnicas que utilizan las botnets evolucionan y se adaptan de manera constante en respuesta a medidas de mitigación.
- Las botnets se han convertido en herramientas populares para los cibercriminales dado que son fáciles de instalar y operar, difíciles de descubrir, y baratas para adquirir o alquilar a través de redes criminales.[2]
- Los creadores y operadores de botnets están geográficamente dispersos de sus bots y son hábiles a la hora de ocultar su ubicación e identidad.
- Hay computadoras vulnerables conectadas a Internet (por ejemplo, aquellas sin un nivel de seguridad adecuado o cuyos usuarios puedan ser tentados a introducir malware tipo botnet en sus equipos). Los operadores de botnets buscan activamente sistemas vulnerables para infectarlos.
- Las botnets están diseñadas para aprovechar propiedades fundamentales del Internet (las llamadas Invariancias del Internet [3]) y su arquitectura, donde la inteligencia esta en los dispositivos finales (por ejemplo, en los servidores de mando y control de las botnets y las computadoras infectadas), no en la propia red.

[2] Ver ejemplos en http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime y http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/

[3] Ver Invariantes de Internet: Lo que realmente importa, http://www.internetsociety.org/internet-invariants-what-really-matters

Principios rectores

La Internet Society cree que un enfoque de colaboración entre todas las partes interesadas permitirá lograr las mejores soluciones para mitigar botnets y proteger la seguridad. Este enfoque se materializa en los principios de Seguridad Colaborativa de la Internet Society, que hacen hincapié en la responsabilidad compartida y colectiva para lograr los resultados deseados.[4] La Seguridad Colaborativa comprende los siguientes principios:

Fomentar la confianza y aprovechar las oportunidades. El objetivo de la seguridad es promover la confianza en Internet y asegurar la continuidad de su éxito como motor de innovación económica y social.

- *Promover la concientización.* Promover una toma de conciencia generalizada de que las partes interesadas se hayan comprometido a trabajar juntas para eliminar y desalentar la creación de nuevas botnets por medio de medidas eficaces, eficientes y razonables.
- *Promover sistemas seguros.* Promover una experiencia en Internet más segura para los usuarios, fomentando prácticas seguras de diseño de software, componentes de seguridad comunes de alta calidad, detección oportuna de vulnerabilidades, suministro de actualizaciones y sistemas similares.
- *Promover dispositivos seguros.* Promover el uso de sistemas que estén correctamente configurados para evitar su infección por malware de botnets. Por ejemplo, a nivel de computadora individual, el uso de protección antimalware y software de detección de spyware reduce el riesgo de infección por botnets.
- *Promover la contención.* Promover una mejora de la capacidad técnica de la comunidad de Internet en general para así contener la propagación, la operación y el impacto de las botnets. Esto incluye mejorar las habilidades para desactivar botnets de manera de reducir sus daños.

Responsabilidad colectiva. Quienes participan de Internet comparten la responsabilidad del sistema como un todo.

- *Responsabilidad compartida.* Todas las partes involucradas se deben esforzar por compartir la responsabilidad de hacer frente a las botnets, entre ellas los gobiernos, los operadores de red, los proveedores de software, los proveedores de servicios en línea, la comunidad técnica y los usuarios finales. Por ejemplo, una red que inadvertidamente aloje una botnet no se vea afectada directamente, el operador de la red debe ser responsable de prevenir que no se convierta en una plataforma de lanzamiento de actividades maliciosas [5] En términos generales, confiar en que unas pocas partes implementen políticas antibotnet o imponer artificialmente responsabilidades legales; en lugar de aplicar un enfoque colectivo, le impone a algunos una carga injusta y podría, potencialmente, alterar el modelo de responsabilidad compartida de Internet.
- *Enfoque colaborativo.* Las actividades colaborativas son esenciales a la hora de tratar con redes de bots. Esto incluye el intercambio de inteligencia y datos operacionales de los ataques, el intercambio de buenas prácticas y métodos de mitigación; además de la coordinación de actividades antibotnet. También es importante que la colaboración sea proactiva y no reactiva.
- *Colaboración transfronteriza.* La colaboración transfronteriza puede ser facilitada por leyes que penalicen criminalicen las botnets y su actividad maliciosa permitan la recolección y el intercambio de información adecuada, para su mitigación y persecución criminal. Se debe prestar especial atención a la implementación de medidas técnicas que permiten detectar y mitigar las botnets a través de las fronteras, quiénes están implicados, y qué es razonable y admisible.

[4] Principios de Seguridad Colaborativa de la Internet Society, http://www.internetsociety.org/collaborativesecurity
[5] Ver https://www.m3aawg.org/abcs-for-ISP-code

Propiedades y valores fundamentales. Las soluciones de seguridad deben ser compatibles con los derechos humanos fundamentales y preservar las propiedades fundamentales de Internet, es decir, los invariantes de Internet.

- *Respetar los derechos de los usuarios.* Al aplicar medidas para abordar las botnets, los enfoques de políticas deben tener en cuenta posibles efectos no deseados sobre el acceso y la privacidad de los usuarios. Algunas soluciones bien intencionadas podrían, inadvertidamente, afectar usos legítimos de Internet o exponer innecesariamente información privada de los usuarios.
- *Preservar las propiedades fundamentales de Internet.* Los enfoques de política deben tener en cuenta el potencial impacto sobre la arquitectura que subyace a Internet y garantizar que no tengan un impacto negativo en la apertura, la innovación sin permiso o el alcance global de Internet. Por ejemplo, dar de baja un dominio podría hacer que algunos sitios web legítimos no infectados quedaran inalcanzables.[6]

Evolución y consenso. Una seguridad eficaz depende de pasos evolutivos ágiles que se basen en la experiencia de un amplio conjunto de partes interesadas.

- *Agilidad.* Dada la rápida evolución de las botnets, las políticas y soluciones deben ser lo suficientemente ágiles como para mantener su eficacia. Por ejemplo, las políticas que impiden que los expertos en seguridad investiguen la conducta de las botnets podrían retrasar el desarrollo de nuevas herramientas y técnicas antibotnet. Además, las políticas deben tratar de abordar la creación, propagación y funcionamiento de los bots y los servidores de mando y control, así como las personas que son sus dueños y las operan.
- *Soluciones tecnológicamente neutras.* Los enfoques a largo plazo se deben diseñar de modo que sean tecnológicamente neutros, es decir, que no prescriban una solución técnica detallada. Por el contrario, las soluciones deben especificar una estrategia general, permitiendo así que la implementación detallada se pueda adaptar a las nuevas tecnologías.
- *Enfocarse en las causas de fondo.* Las estrategias deben enfocarse en la causa que se encuentra en la raíz del problema. Si se abordan los síntomas (por ejemplo, el correo no deseado) sin abordar también la causa de fondo (la botnet) se podrían descuidar otras actividades maliciosas de las botnets (por ejemplo, el robo de datos personales).
- *Soluciones parciales.* Los formuladores de políticas deben tener en cuenta que las soluciones parciales para combatir las botnets podrían tener su mérito. Las medidas progresivas para la detección y desactivación de botnets no eliminan por completo la amenaza, pero sí ayudan a contener el problema y disminuyen la rentabilidad de las botnets.

Pensar a nivel global, actuar a nivel local. Es probable que la mejor forma de llegar a las soluciones más eficaces sea a través de una auto organización de abajo hacia arriba.

- *Generar confianza.* En general, las estrategias más efectivas contra las botnets son implementadas por grupos informales auto organizados que se construyen en base a la confianza que existe entre los expertos en la materia.[7]

[6] Ver, por ejemplo, http://www.pcworld.com/article/2452460/microsoft-settles-with-noip-in-botnet-hunt-after-seizing-its-domains.html
[7] Ver, por ejemplo, http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836

Recursos adicionales

La Internet Society ha publicado una serie de documentos y contenido adicional relacionado con este tema. Se puede acceder libremente a estos materiales en nuestro sitio web.

- Seguridad colaborativa. Un enfoque para abordar cuestiones de seguridad en Internet, http://www.internetsociety.org/collaborativesecurity
- Colaboración global de múltiples partes interesadas para lograr un ciberespacio seguro y tolerante: crecimiento y desarrollo sostenible a través de la cibernética, http://internetsociety.org/doc/global-multi-stakeholder-collaboration-achieving-safe-secure-and-tolerant-cyberspace-enabling
- Seguridad y resiliencia de Internet, http://www.internetsociety.org/doc/understanding-security-and-resilience-internet, e infografía: Colaboración para una Internet segura y resiliente, http://internetsociety.org/doc/infographic-collaboration-secure-and-resilient-internet
- Ciberseguridad: armando el rompecabezas de la ciberseguridad, http://internetsociety.org/cybersecurity-laying-out-pieces-cybersecurity-puzzle
- Hacia una mejora de la seguridad, estabilidad y resiliencia del DNS, http://internetsociety.org/towards-improving-dns-security-stability-and-resiliency-0

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444 • Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tel: +1 703 439 2120 • Fax: +1 703 326 9881
Correo electrónico: info@isoc.org

bp-botnets-20151030-es