¿Qué es una red de robots (botnet) de DDoS?

Los ataques de redes de robots (botnet) son responsables de los mayores ataques DDoS registrados. Descubre cómo se infectan los dispositivos con malware (software malicioso) de redes de robots (botnet), cómo se controlan los robots de manera remota y cómo proteger una red de una infestación de red de robots (botnet).

Metas de aprendizaje

Después de leer este artículo podrás:

- Definir una red de robots (botnet) DDoS
- Explicar por qué se crearon las redes de robots (botnets)
- Comprender cómo los atacantes controlan de manera remota las redes de robots (botnets)
- Razonar sobre las estrategias para inhabilitar una red de robots (botnet) y evitar infecciones

CONTENIDO RELACIONADO

¿Qué es un ataque de denegación de servicio (DoS)?

Modelo OSI

¿Qué es el enrutamiento de agujeros negros de DDoS?

Mitigación de DDoS

Cómo lanzar un ataque DDoS | Herramientas de ataque DoS y DDoS

¿Quieres saber más?

Suscríbete a theNET, el resumen mensual de Cloudflare sobre las ideas más populares de Internet.

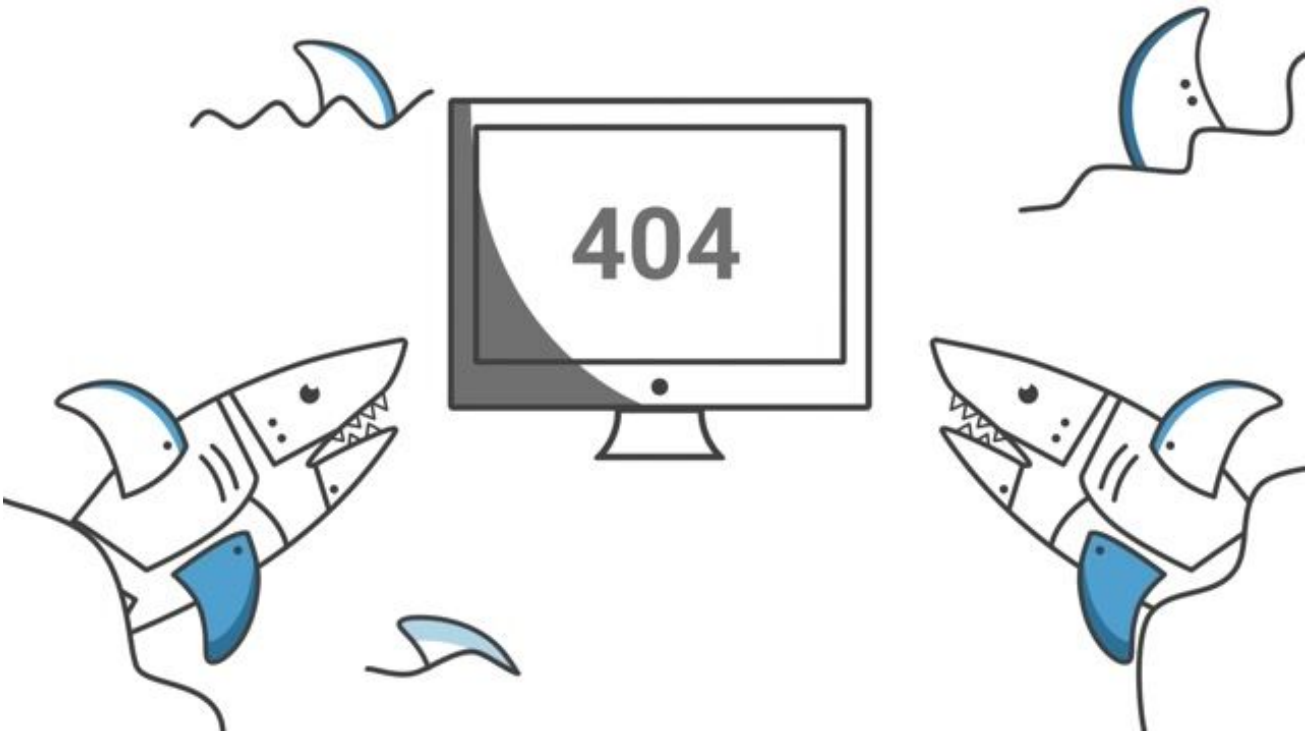
Correo electrónico: *

Suscripción a theNET

Revisa la política de privacidad de Cloudflare para saber más sobre cómo Cloudflare gestiona tus datos personales.

Copiar el enlace del artículo

¿Qué es una botnet?

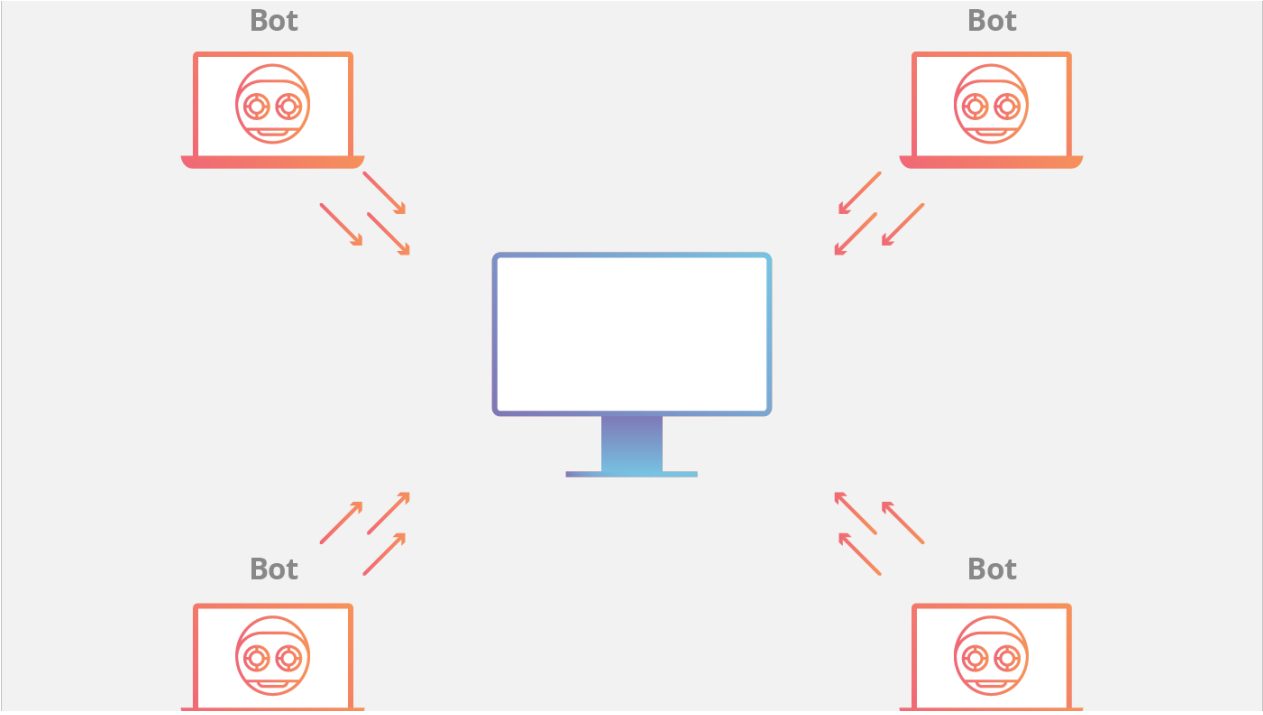


Una red de bots (botnet) es un grupo de computadoras que han sido infectadas por malware (software malicioso) y que han quedado bajo el control del actor malicioso. El término botnet es una combinación de las palabras bot y "network" (red), y cada dispositivo infectado se llama bot. Las redes de bots (botnets) pueden diseñarse para llevar a cabo tareas ilegales o maliciosas, como el envío de correo no deseado, el robo de datos, el ransomware, los clics fraudulentos en anuncios o los ataques de denegación de servicio distribuido (DDoS).

Si bien algunos malware (software malicioso), como el ransomware, tendrán un impacto directo sobre el propietario del dispositivo, el malware de las redes de bots (botnets) puede tener distintos niveles de visibilidad. Algunos malware están diseñados para tomar el control de un dispositivo, mientras que otros se ejecutan en silencio como un proceso de fondo y esperan instrucciones del atacante o "pastor de bots".

Las redes de bots (botnets) que se propagan automáticamente reclutan bots adicionales a través de una variedad de canales. Las vías para la infección incluyen la explotación de las vulnerabilidades de los sitios web, el malware (software malicioso) troyano y la averiguación de autenticaciones débiles para obtener acceso remoto. Una vez que se obtiene acceso, todos estos métodos de infección provocan la instalación del malware (software malicioso) en el dispositivo fijado como objetivo y habilitan el control remoto por parte del operador de la red de bots (botnet). Cuando se ha infectado un dispositivo, este puede intentar propagar el malware (software malicioso) de la red de bots (botnet) al reclutar otros dispositivos de hardware en la red circundante.

Si bien es imposible precisar la cantidad exacta de robots en una red de robots (botnet) particular, para el número total de robots en una red sofisticada se han estimado entre miles a más de un millón.



¿Por qué se crean las redes de robots (botnets)?

Las razones para usar una red de robots (botnet) van desde el activismo hasta la interrupción patrocinada por el estado. Además, muchos ataques se llevan a cabo solo para ganar dinero. Contratar servicios de redes de robots (botnets) en línea es relativamente asequible, en especial si se considera el daño que pueden causar. La barrera para crear una red de robots (botnet) también es lo suficientemente baja como para que algunos desarrolladores de software hagan un negocio lucrativo, especialmente en ubicaciones geográficas donde la regulación y la justicia son limitadas. Esta combinación ha llevado a la proliferación de los servicios en línea que ofrecen ataques por encargo.

¿Cómo se controla una red de robots (botnet)?

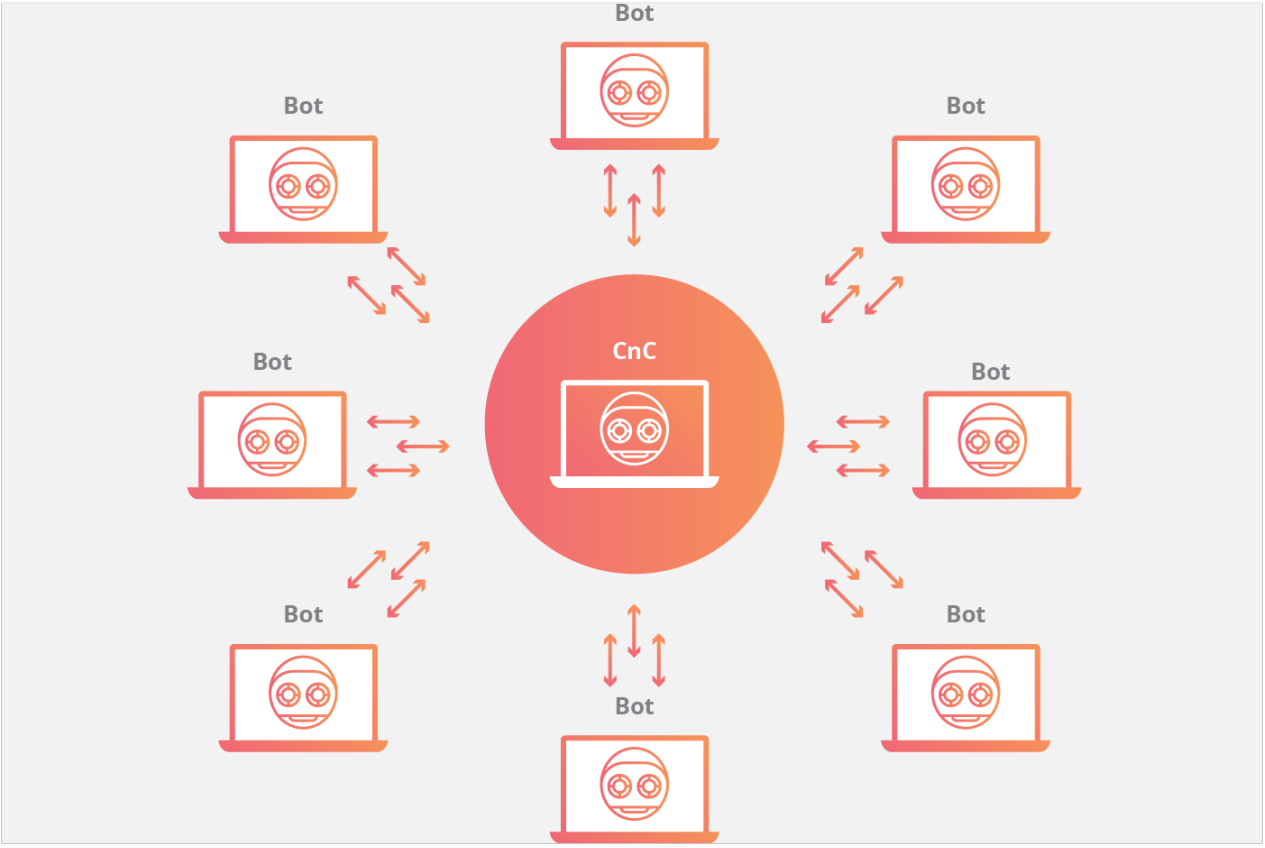
Una característica central de una red de bots (botnet) es la capacidad para recibir instrucciones actualizadas del pastor de bots. Poder comunicarse con cada bot de la red permite al atacante alternar los vectores de ataque, cambiar la dirección IP que se fija como objetivo, finalizar el ataque y llevar a cabo otras acciones personalizadas. Los diseños de redes de bots (botnets) varían, pero las estructuras de control pueden dividirse en dos categorías generales:

El modelo de red de robots (botnet) cliente-servidor

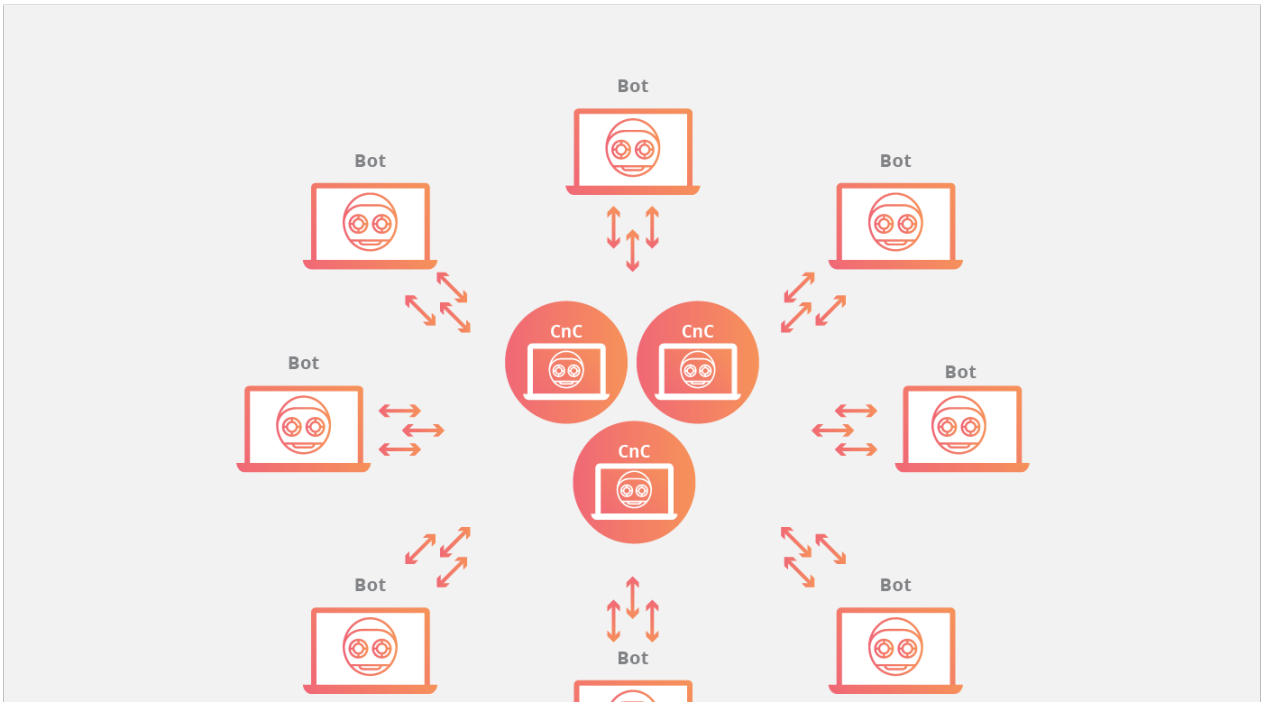
El modelo cliente-servidor imita el flujo de trabajo de la estación de trabajo remota tradicional, en la que cada máquina individual se conecta a un servidor centralizado (o un número reducido de servidores centralizados) para acceder a la información. En este modelo, cada bot se conectará a un recurso del centro de comando y control (CnC) como un dominio web o un canal IRC para recibir instrucciones. Al usar estos repositorios centralizados para entregar comandos nuevos para la red de bots (botnet), un atacante solo necesita modificar el material original que cada red de bots (botnet) consume de un centro de comando para actualizar las instrucciones a las máquinas infectadas. El servidor centralizado que controla la red de bots (botnet) puede ser un dispositivo perteneciente al atacante y operado por este, o bien un dispositivo infectado.

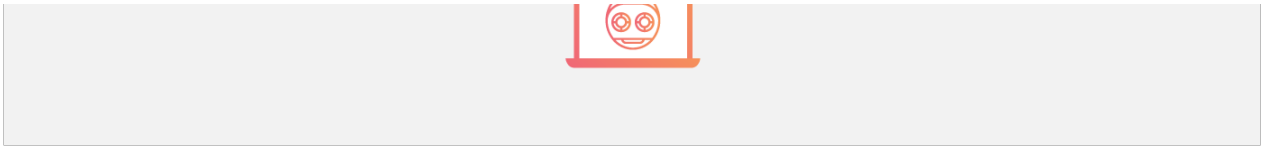
Se ha observado un número de topologías de redes de robots (botnets) centralizadas populares, incluidas las siguientes:

Topología de red en estrella

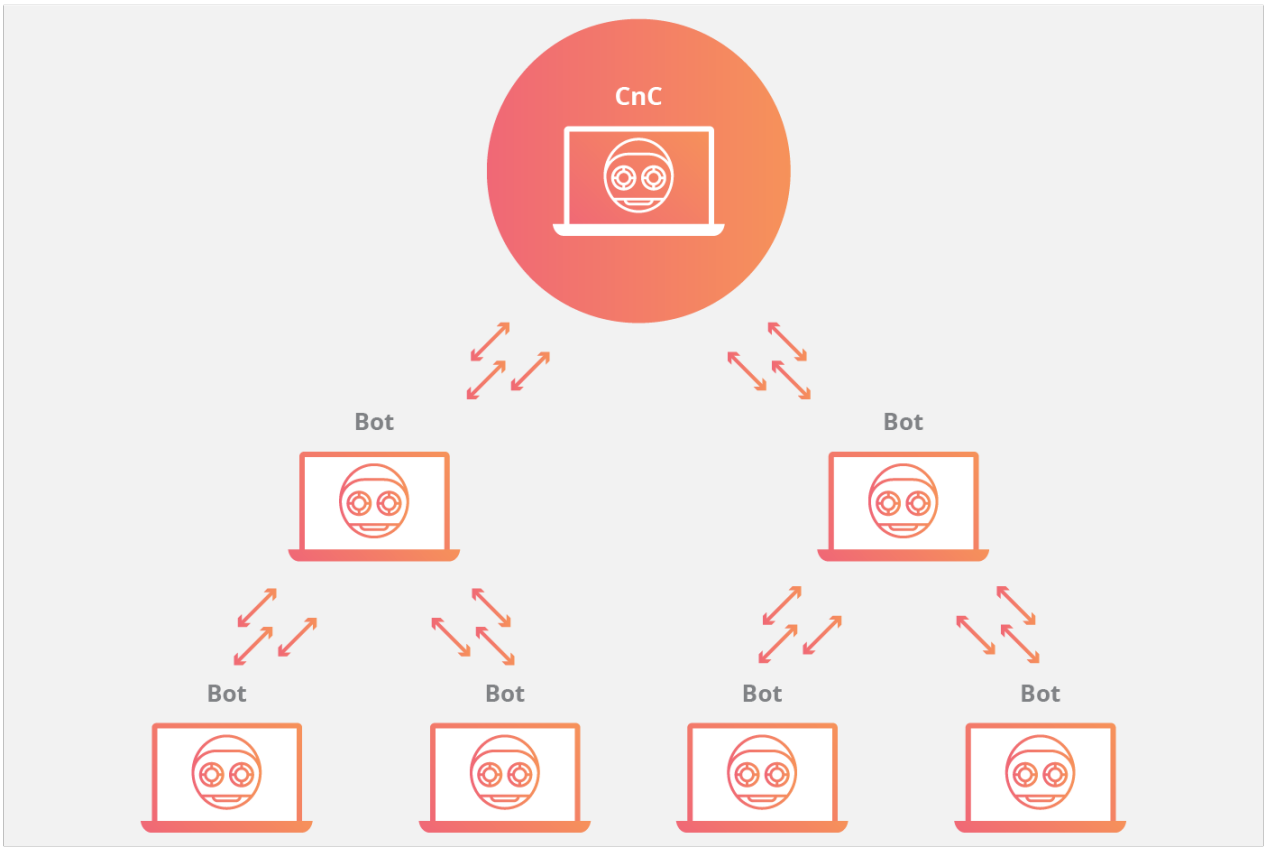


Topología de red de servidores múltiples





Topología de red jerárquica



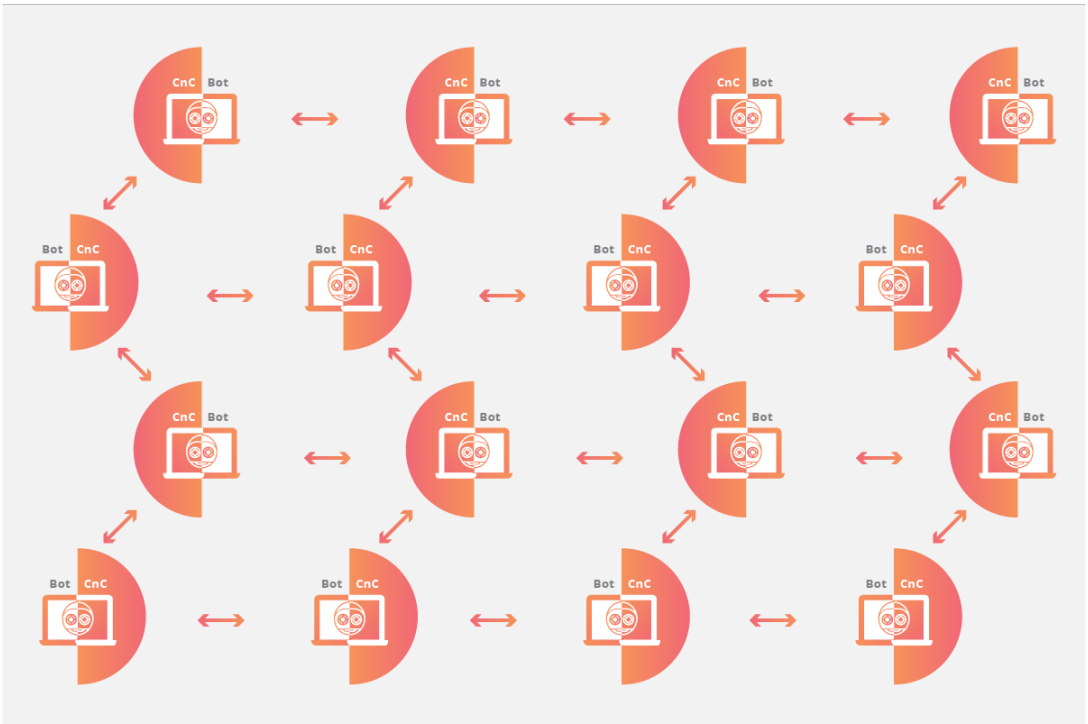
En cualquiera de estos modelos cliente-servidor, cada bot se conectará a un recurso del centro de comando como un dominio web o un canal IRC para recibir instrucciones. Al usar estos repositorios centralizados para entregar comandos nuevos para la red de robots (botnet), un atacante solo necesita modificar el material original que cada red de robots (botnet) consume de un centro de comando para actualizar las instrucciones a las máquinas infectadas.

A la par de la simpleza de actualizar instrucciones a la red de robots (botnet) desde una cantidad limitada de fuentes centralizadas se encuentra la vulnerabilidad de esas máquinas. Para eliminar una red de robots (botnet) con un servidor centralizado, solo necesita interrumpirse el servidor. Como resultado de esta vulnerabilidad, los creadores del malware (software malicioso) de la red de robots (botnet) han evolucionado y avanzado hacia un modelo nuevo que es menos susceptible a la interrupción mediante uno o varios puntos de error.

El modelo de la red de robots (botnet) entre pares

Para evadir las vulnerabilidades del modelo cliente-servidor, recientemente se han diseñado redes de robots (botnets) mediante el uso de componentes del intercambio de archivos descentralizado. Insertar la estructura de control dentro de la red de robots (botnet) elimina el único punto de error presente en una red de robots (botnet) con servidor centralizado, lo que dificulta los esfuerzos de mitigación. Los bots P2P (entre pares) pueden ser clientes y centros de comando que trabajan codo a codo con sus nodos vecinos para propagar datos.

Las redes de robots (botnets) entre pares mantienen una lista de computadoras confiables con las cuales pueden enviar y recibir comunicaciones y actualizar su malware (software malicioso). Al limitar el número de máquinas a las que se conecta el bot, cada bot se expone solo a dispositivos adyacentes, lo cual dificulta el rastreo y la mitigación. No contar con un servidor de comando centralizado hace a las redes de robots (botnet) entre pares más vulnerables al control de alguien que no sea su creador. Para proteger contra la pérdida de control, las redes de robots (botnets) descentralizadas suelen estar cifradas para que el acceso sea limitado.



¿Cómo se convierten los dispositivos IoT en una red de robots (botnet)?

Nadie hace operaciones bancarias en Internet a través de la cámara CCTV inalámbrica que se encuentra en el jardín para observar el comedero de pájaros. Sin embargo, esto no significa que el dispositivo no pueda hacer las solicitudes de red necesarias. El poder de los dispositivos IoT junto con la seguridad débil o mal configurada crea una entrada para que el malware (software malicioso) de la red de bots (botnet) reclute bots nuevos para el colectivo. El aumento de los dispositivos IoT ha dado lugar a un nuevo panorama de ataques DDoS, ya que muchos dispositivos están mal configurados y son vulnerables.

Si la vulnerabilidad de un dispositivo IoT está codificado en firmware, las actualizaciones son más difíciles. Para mitigar el riesgo, los dispositivos IoT con firmware obsoleto deben actualizarse, ya que las credenciales predeterminadas no suelen cambiar desde la instalación inicial del dispositivo. Muchos fabricantes de hardware más económico no tienen el incentivo para hacer más seguros sus dispositivos, lo que provoca que la vulnerabilidad que representa el malware (software malicioso) de redes de robots (botnets) para los dispositivos IoT siga siendo un riesgo de seguridad sin resolver.

¿Cómo se deshabilita una red de robots (botnet) existente?

Deshabilita los centros de control de una red de robots (botnet):

Las redes de robots (botnets) diseñadas mediante un esquema de comando y control pueden deshabilitarse con más facilidad después de identificar los centros de control. Cortar de raíz los puntos de error puede desconectar toda la red de robots (botnet). Como resultado, los administradores de sistemas y oficiales de las fuerzas de seguridad se enfocan en cerrar los centros de control de esas redes de robots (botnets). Este proceso es más difícil si el centro de comando opera en un país donde las fuerzas de seguridad tiene menos capacidad o disposición para intervenir.

Elimina la infección en dispositivos individuales:

Para las computadoras individuales, las estrategias para recuperar el control de las

máquinas incluyen ejecutar software de antivirus, reinstalar el software desde una copia de seguridad o comenzar de nuevo desde una máquina limpia tras formatear el sistema. Para los dispositivos IoT, las estrategias pueden incluir intercambiar el firmware, ejecutar un restablecimiento de fábrica o formatear el dispositivo. Si estas opciones no son viables, el fabricante del dispositivo o el administrador del sistema puede ofrecer otras estrategias disponibles.

¿Cómo puedes proteger los dispositivos para que no sean parte de una red de robots (botnet)?

Crea contraseñas seguras:

Para muchos dispositivos vulnerables, reducir la exposición a la vulnerabilidad de la botnet puede ser tan simple como cambiar las credenciales administrativas por otras que no sean el nombre de usuario y la contraseña predeterminadas. Crear una contraseña segura dificulta la decodificación por fuerza bruta, por lo que crear una contraseña muy segura hace que la decodificación por fuerza bruta sea prácticamente imposible. Por ejemplo, un dispositivo infectado con el malware Mirai escaneará las direcciones IP en busca de dispositivos que respondan. Una vez que un dispositivo responde a una solicitud de ping, el bot intentará iniciar sesión en ese dispositivo encontrado mediante el uso de una lista de credenciales predeterminadas. Si se ha cambiado la contraseña predeterminada y se ha implementado una contraseña segura, el bot se rendirá y seguirá buscando otros dispositivos vulnerables.

Permite solo la ejecución confiable de códigos de terceros:

Si adoptas el modelo de ejecución de software de teléfono móvil, pueden ejecutarse solo las aplicaciones en la lista blanca. Esto brinda más control para acabar con el software considerado malicioso, incluidas las redes de bots (botnets). Solo una explotación del software del supervisor (tal como kernel) puede causar la explotación del dispositivo. En primer lugar, esto depende de contar con un kernel seguro, que la mayoría de los dispositivos IoT no tienen, y es más aplicable a máquinas que ejecutan software de terceros.

Borra o restaura sistemas periódicamente:

Restaurar el sistema a un buen estado después de un tiempo predeterminado eliminará cualquier suciedad que haya recolectado un sistema, incluido el software de red de robots (botnet). Esta estrategia, cuando se usa como medida preventiva, asegura que se elimine incluso el malware (software malicioso) ejecutado en silencio.

Implementa buenas prácticas de filtrado de entrada y salida:

Otras estrategias más avanzadas incluyen prácticas de filtrado en los routers y firewalls de la red. Un principio del diseño de red seguro es disponer capas: tienes la restricción mínima alrededor de los recursos accesibles al público y fortaleces la seguridad constantemente para los archivos que consideres confidenciales. Además, todo lo que cruce estos límites debe pasar por un escrutinio: tráfico de red, unidades USB, etc. Las prácticas de filtrado de calidad aumentan la probabilidad de que se atrapen el malware (software malicioso) DDoS y sus métodos de propagación y comunicación antes de entrar o salir de la red.

Si actualmente eres víctima de un ataque, puedes tomar medidas para combatirlo. Si ya cuentas con Cloudflare, puedes seguir estos pasos para mitigar el ataque. La protección contra ataques DDoS que implementamos en Cloudflare es multidimensional con el fin de mitigar los posibles vectores de ataque. Más información sobre la protección DDoS de Cloudflare.

Primeros pasos

Planes gratuitos

Para empresas

Compara planes

Búsqueda de nombres de dominio

Sugerencias

Solicitar demostración

Contacta con Ventas

Acerca de los ataques DDoS

Ataques DDoS

Herramientas de ataque DDoS

Glosario de DDoS

Navegación del centro de aprendizaje