Dirección Nacional
de Ciberseguridad

Botnets

Una guía y un glosario para entender su funcionamiento

Argentina unida

Jefatura de
Gabinete de Ministros
Argentina

Secretaría de
Innovación Pública

Introducción

Las botnets son una serie de dispositivos informáticos que realizan tareas programadas en forma conjunta, algunas con fines lícitos y otras ilícitos, es decir, que son maliciosas.

Las de fines lícitos se pueden utilizar por ejemplo para tareas de seguridad informática, como la realización de pentests, que son manejadas desde el comando y control por un especialista o profesional del sector.

Las botnets usadas para fines ilícitos se arman sin el conocimiento de que varios dispositivos (computadoras, celulares, tablets, etc) son parte de las mismas.

Entonces, una botnet es una **red de dispositivos capaces de conectarse a Internet**, que es controlada de manera remota y funciona de forma autónoma y automática. En las de uso malicioso, funcionan sin la autorización ni el conocimiento de las personas usuarias de esos dispositivos.

Las botnets también son conocidas como redes de **computadoras zombis** que se utilizan para realizar tareas rutinarias, pesadas y automáticas que le son asignadas por quien las controla.

En la actualidad, las botnets tienen entre sus blancos a dispositivos de **Internet de las Cosas** (IoT, por su sigla en inglés). Un claro ejemplo es la botnet Mirai, que genera un interés cada vez mayor por parte de aquellos atacantes que apuntan a vulnerabilidades más antiguas en productos de IoT para el mercado consumidor dado que los ciberdelincuentes saben que los dispositivos de IoT están menos protegidos y buscan aprovechar esa vulnerabilidad.

Además, existen otras botnets que siguen activas en la región como lo son los casos de **Gh0st y Andromeda**, también conocidas como Gamaru y Wauchos.

Para defenderse de este tipo de ataques, que también pueden afectar a computadoras de escritorio y notebooks, es necesario poner en conocimiento sobre cómo funcionan las botnets. Desde la **Dirección Nacional de Ciberseguridad**, dependiente de la **Subsecretaría de Tecnologías de la Información y las Comunicaciones de la Secretaría de Innovación Pública**, se elaboró un informe con los principales datos que hay que tener en cuenta sobre las botnets.

En esta breve guía se propone explicar de qué se tratan las botnets y cuáles han sido los casos más resonantes que afectaron sistemas.

Definiciones para entender

Las botnets son una serie de dispositivos informáticos que realizan tareas programadas en forma conjunta, algunas con fines lícitos y otras ilícitos, es decir, que son maliciosas.

Las de fines lícitos se pueden utilizar por ejemplo para tareas de seguridad informática, como la realización de pentests, que son manejadas desde el comando y control por un especialista o profesional del sector.

Las botnets usadas para fines ilícitos se arman sin el conocimiento de que varios dispositivos (computadoras, celulares, tablets, etc) son parte de las mismas.

Entonces, una botnet es una **red de dispositivos capaces de conectarse a Internet**, que es controlada de manera remota y funciona de forma autónoma y automática. En las de uso malicioso, funcionan sin la autorización ni el conocimiento de las personas usuarias de esos dispositivos.

Las botnets también son conocidas como redes de **computadoras zombis** que se utilizan para realizar tareas rutinarias, pesadas y automáticas que le son asignadas por quien las controla.

En este caso particular de ataque, quien las comanda es conocido como **“bot herder”**, algo así como **“pastor de robots”**, aunque esta expresión no guarda ningún tipo de relación con la de robots zombis.

Su nombre deviene de **“bot”**, apócope de robot informático y **“net”**, red en inglés, y fue utilizado por primera vez en 2001 en el proceso judicial que EarthLink Inc. sostuvo contra Khan C. Smith, quien había montado una botnet para el envío de correo electrónico no deseado.

Si bien las primeras botnets estaban compuestas por computadoras de escritorio y portátiles, con el aceleramiento en la capacidad de procesamiento de los dispositivos, rápidamente las tabletas y los teléfonos inteligentes se sumaron a la lista de blancos. Pues bien, el futuro llegó hace rato, ya en el año 2013 un investigador de la compañía de seguridad corporativa Proofpoint detectó una botnet que incluía televisores inteligentes, heladeras y otros electrodomésticos “smart”. Esto se debe al avance de la llamada **Internet de las Cosas** (IoT), que no es otra cosa que la capacidad de conectar objetos tan disímiles como autos y relojes a la web.

¿Cómo se crea una botnet?

Existen muchas maneras de formar una de estas redes pero la más difundida es a través de la distribución de software malicioso o malware, que instala en el dispositivo el programa que permite controlar las funciones deseadas a través del aprovechamiento de las vulnerabilidades del sistema operativo o bien engañando a la persona usuaria.

Por lo general, el método utilizado para infectar dispositivos es el troyano, un software que se presenta ante la persona usuaria como legítimo y seguro pero que en realidad tiene por objetivo sacar algún tipo de provecho del dispositivo o de la persona. La manera en la que este tipo de malware se cuela en el sistema puede entenderse a través de la analogía con el Caballo de Troya, mencionado por primera vez en el poema épico de Homero, La Odisea.

Así, una vez que el hacker toma control del equipo a través de este u otros artilugios, está en condiciones de añadir un nuevo zombi a su red, o bien puede hacer que el malware permanezca latente, y por tanto más difícil de detectar, hasta el momento en que decida activarlo para el ataque.

¿Cómo funcionan las botnets?

Las botnets suelen utilizar servicios gratuitos de DNS, aunque por supuesto existen redes tejidas de manera más consistente y refinada y que poseen servidores de reemplazo en caso de cualquier “inconveniente”. En el pasado el control de estas redes se ejercía mediante la utilización de IRC pero con el tiempo se ha mudado su comando hacia diversos protocolos volviendo más dificultosa su detección.

Sin abundar en tecnicismos es importante entender que el funcionamiento de una botnet consiste en utilizar parte de la capacidad de procesamiento de los dispositivos que la componen para realizar diversas tareas que van desde el envío de correo masivo, la denegación de servicio (DDoS), minar Bitcoins o cualquier otra actividad que genere un beneficio para el “Bot herder”. Aunque esto será detallado más adelante.

Tipos de Botnet

En función de las formas de configuración de estas redes podemos distinguir fundamentalmente dos grandes tipos: el de cliente-servidor y el de peer-to-peer.

Cliente-servidor

Se trata de la forma primigenia en la que el hacker se contactaba con las computadoras zombis para ordenarles las tareas a realizar. Esta forma de comunicación se basa en una única ubicación de origen, generalmente un sitio web o un servidor. Como toda forma primigenia ha evolucionado, pero si bien a través de esta metodología es relativamente sencillo crear una red de robots zombis, también lo es detectarla y darla de baja.

Punto a punto (p2p)

Esta nueva forma de organización de botnets surgió de la necesidad de los hackers de eliminar la principal debilidad de dichas redes. Así, cada equipo infectado se comunica de forma directa con sus "compañeros", de modo que eliminar a uno o varios "soldados" del ejército zombi, implicará una merma en la capacidad de procesamiento de la red pero no su eliminación.

Usos más frecuentes de las botnets

Para entender los usos que se les dan a estas redes podemos valernos de uno de los nombres por los que se le conoce: red de robots zombis. Este tipo de redes funcionará con las características de una horda de las películas de George Romero, es decir, los dispositivos afectados no podrán realizar grandes acciones de forma individual, su fortaleza no se encuentra en su brillantez o habilidades sino en la sumatoria de ingentes cantidades de sistemas trabajando como bloque. En función de esta naturaleza tan marcada, estas redes de sistemas zombis son utilizadas para enviar paquetes en forma masiva y veloz o lograr que todos los dispositivos hagan lo mismo a la vez. En lo simple de la idea está también lo implacable de su efecto. Veamos, aunque en forma superficial, alguno de los usos más comunes que han recibido estas redes.

Envío de correo electrónico masivo (SPAM)

Una tarea muy sencilla a realizar por un grupo de dispositivos es asignarle una lista de direcciones, un bolso con paquetes y lanzarlos a las calles digitales como carteros. Este fue el primer uso que recibieron las botnets: repartir correos no deseados al contar con millones de computadoras que los propaguen de manera mecánica y lleguen a tantas personas como sea posible.

Distribución de malware

Al tener a disposición una red capaz de enviar de forma masiva correos electrónicos no deseados, los hackers no tardaron en utilizarlas para distribuir elementos más perjudiciales. Así como la finalidad del SPAM es llegar a la mayor cantidad de destinos posible, lo mismo sucede con el malware, con el agregado de que la velocidad tiene una importancia estratégica.

Este tipo de software suele ser detectado en el ciberespacio de manera relativamente veloz y las actualizaciones de las bases de datos de los antivirus salen a su cruce con toda la celeridad posible. Así, la velocidad en la distribución del software maligno es clave para su éxito, y la multiplicidad de dispositivos que lo distribuyen cumplen esta tarea con frialdad pasmosa.

Ataque de denegación de servicio DDoS

Sigamos con la metáfora de los dispositivos zombis. Es probable que un individuo, o dispositivo, que goce de buena salud pueda evadir o repeler a una de estas criaturas, pero si en lugar de una se tratase de una cantidad suficiente como para que la suma de sus fuerzas lo supere ampliamente, la situación es muy otra. Un ataque de denegación de servicio consiste en lograr que un número suficiente de "zombis" le envíe determinados pedidos a un sitio web con la finalidad de ralentizarlo mucho o directamente hacer colapsar su capacidad de respuesta.

Robar contraseñas a través de la fuerza bruta

Existen muchas maneras de hackear una cuenta, sea de correo electrónico, de perfil en redes sociales, home banking o cualquier otro sistema que exija loguearse. Aún cuando la persona usuaria cree contraseñas con características de cierta fortaleza, hay una manera de lograr entrar y ésta no presupone el conocimiento de ninguna de las ideas de quien la creó.

Un ataque de fuerza bruta consiste en intentar todas las combinaciones de letras, números y caracteres especiales hasta dar con la correcta, así de ciego y bruto como se lee. Recordemos que una de las principales características de una botnet es la capacidad de realizar una tarea mecánica, repetitiva y tediosa de manera automática.

Para evitar este tipo de ataques es que de un tiempo a esta parte los sitios web y dispositivos electrónicos sólo permiten un número limitado de intentos de logueo. Aquí viene la clave de la frialdad de la botnet, al tener múltiples sistemas intentando ingresar, pueden ir siendo bloqueados uno a uno pero siempre habrá otro *"zombi"* detrás esperando a acertar la combinación o ser bloqueado al agotar su número de intentos. Es una batalla de desgaste y con una red lo suficientemente grande y tiempo disponible, cualquier sistema a la larga colapsa.

Generar ingresos a través de minar Bitcoins

El perjuicio para la persona usuaria puede variar desde la molestia por el correo no deseado, la amenaza de recibir malware o el robo de una cuenta de servicio digital, pero también puede ser que de su dispositivo se "distraiga" una parte de la capacidad de procesamiento para "minar Bitcoins" u otras criptomonedas. Un equipo de una persona usuaria utilizado para esta actividad se ralentizará enormemente, al tiempo que elevará su consumo de electricidad y acelerará los tiempos de desgaste del dispositivo, más aún en aquellos que utilicen batería. Para darse una idea de la magnitud de esto basta pensar que si la "minería de bitcoin" fuese

un país, consumiría al año más electricidad que la República Argentina. Y todo esto sin contar su influencia en la dificultad para conseguir y el aumento de precio de las placas aceleradoras de video.

Los casos más resonantes

En el tiempo que internet se ha vuelto un elemento de consumo global y masivo ha habido varios casos notables de este tipo de ataques cibernéticos. Haremos un recorrido sintético por algunos de los más resonantes.

GAmeover ZeuS

Se trató de una botnet de modelo peer-to-peer creada luego del troyano Zeus y que tuvo un devastador punto de partida ya que este malware había infectado a más de 3.600.000 dispositivos. Luego de una exhaustiva investigación del FBI detuvieron a más de cien personas en todo el mundo.

Esta botnet se basó en una red cifrada que dificultó notablemente su detección, estaba dirigida al sistema operativo Windows y distribuyó el ransomware **“Cryptolocker”** y una serie de estafas bancarias fraudulentas. Un ransomware es un tipo específico de malware mediante el cual el ciberdelincuente toma el control del dispositivo infectado y lo “secuestra” en todo o en parte y extorsiona a la persona usuaria, generalmente pidiendo un rescate económico.

Más allá de que la botnet fue desactivada y se realizaron cuantiosos arrestos, el daño ya estaba hecho: se estima que cerca del 1,3 % de las personas usuarias que se infectaron con Cryptolocker pagaron el rescate, lo que reportó ganancias por aproximadamente tres millones de dólares estadounidenses.

Mirai

Diseñada para dirigirse a sistemas Linux, Mirai fue una botnet que se usó para uno de los mayores ataques DDoS de la década, y fue descubierta en el año 2016 por los hackers de sombrero blanco de Malware Must Die. Su rasgo más saliente fue la agresividad con la que se propagaba: una vez que había infectado un equipo podía buscar ingresar a otros dispositivos IoT conectados a la misma red. Así, al detectar un nuevo blanco usaba una base de datos interna de contraseñas y nombres de usuarios predeterminados de fábrica para continuar en procura de nuevas víctimas. ¿Qué es un “hacker de sombrero blanco” o white hat? Es alguien experto en seguridad informática que, para simplificarlo, es la contrapartida de los ciberdelincuentes.

Con predilección por las **"celebridades"**, Mirai atacó la infraestructura de Internet de Liberia, **GitHub, Twitter, Reddit, Netflix y Airbnb**. Se utilizó en muchísimos ataques DDoS. Al basarse en vulnerabilidades de los dispositivos en su configuración predeterminada de fábrica, al actualizar los firmwares de los elementos IoT el malware quedó obsoleto.

Aun así, estuvo en funcionamiento casi dos años antes de que se acabase con él, lo que lo convierte en una de las botnets con mayor "éxito" del mundo aunque también fue una de las menos "maliciosas" ya que evitaba infectar determinados objetivos estratégicos y eliminaba el malware preexistente instalado en los dispositivos, al tiempo que evitaba futuras intrusiones.

ZeroAccess

Un caso curioso, al contrario de lo que su nombre podría indicar, la botnet **ZeroAccess** no participó en ningún ataque DdoS; aunque esto no significa que no se tratase de una red realmente efectiva y peligrosa.

A diferencia del caso anterior donde el método elegido para penetrar los sistemas fue el IoT, **ZeroAccess** se propagó de forma agresiva gracias al uso de ingeniería social y así logró infectar a unos 9 millones de dispositivos. Más allá de esta cifra, la botnet estaba integrada por alrededor de dos millones de equipos, quedando los restantes como una especie de ejército de reserva. El objetivo de **ZeroAccess** no fue otro que minar Bitcoins. Según estimaciones, los creadores de la botnet podrían haber ganado hasta 38 millones de dólares.

Backdoor. Flashback

Entre las personas usuarias de equipos Mac existió durante mucho tiempo la creencia de que no necesitaban instalar sistemas de protección como antivirus o cortafuegos, por más ridículo que esto parezca. Esa asunción se basaba en la idea de que nadie creaba software malicioso destinado a afectar a sus sistemas operativos pues representaban una tasa marginal en relación a Windows y Linux.

Con la irrupción de los teléfonos inteligentes, las tabletas y la masificación de las notebooks Mac en la primera década del siglo XXI la cosa cambió y el troyano **Backdoor.Flashback** afectó a más de 600.000 de estos dispositivos en 2011 y 2012. El impacto no fue menor dado que en función de la creencia antes citada pocas personas usuarias estaban preparadas.

Como una horda de Morlocks capturando a los indolentes Eoi de La Máquina del Tiempo de H.G. Wells, este troyano se valía de una vulnerabilidad de Java, infectaba el dispositivo y lo redirigía a un sitio falso del que se descargaba una serie de malware que convertiría al Mac en un zombi complaciente, además de otro malware problemático que robaría datos personales y ralentizaría el equipo.
La botnet creada, hasta lo que se sabe hoy día, no hizo nada con los datos apropiados ni con el control de los dispositivos subyugados. **Backdoor.Flashback** creó una red punto a punto (p2p) pero sus creadores nunca le "ordenaron" que hiciera nada más allá de reproducirse donde pudiese hasta que fue detenido en 2012. Mucho se especuló con respecto a la no

utilización de esta botnet, la hipótesis con más consenso es que el número de dispositivos infectados no fue suficiente para los planes de los hackers

Perjuicios para la persona usuaria

Ya se ha mencionado anteriormente aunque de manera superficial cuáles son los perjuicios de que un dispositivo integre una botnet pero se pasó por alto la que tal vez sea la principal de las cuestiones: nunca es bueno entregar nuestros dispositivos al control de personas extrañas que por lo general carecen de buenas intenciones. Más allá de las cuestiones puntuales hay que tener en cuenta el alto riesgo que esto implica.

Un dispositivo que forma parte de una botnet está ocupando parte de su capacidad de procesamiento en hacer una tarea que no redunda en beneficio alguno de la persona usuaria. Así, el sistema pierde velocidad, lo que es más notorio cuando se quieren realizar tareas que consuman muchos recursos.

Más grave aún para la persona usuaria es el robo de identidad. Para diversas actividades como el uso envío de SPAM resulta una gran ventaja para los hackers la utilización de una cuenta personal de correo ya que de esta manera se saltan los controles destinados a evitarlo.

El perjuicio económico es otro factor no desdeñable. Esta utilización de recursos no autorizada por la persona usuaria redunda en un mayor consumo de electricidad en el hogar. Y como si fuera poco, si aceptamos que su dispositivo es controlado por una persona extraña, no es difícil arribar a la conclusión de que esto le genera cada vez más vulnerabilidad y exposición a otro tipo de ataques.

Links de referencia

- **INCIBE** (s/f). Glosario de términos de ciberseguridad. www.incibe.es. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf [12 de julio de 2021].
- s/n (31 de octubre de 2018). **"El bitcoin cumple 10 años: qué es y cómo funciona la mayor criptomoneda de la historia"**, BBC News. Recuperado de: https://www.bbc.com/mundo/noticias-46037430 [12 de julio de 2021].
- s/n (22 de febrero de 2021). **"Qué tanto contamina el bitcoin, la moneda que consume más electricidad que Finlandia, Suiza o Argentina"**, BBC News. Recuperado de: https://www.bbc.com/mundo/noticias-56049826 [12 de julio de 2021].
- Eremin, Alexander (2 de abril de 2019). **"Bots y botnets en 2018"**, Securelist. Recuperado de: https://securelist.lat/bots-and-botnets-in-2018/88697/ [12 de julio de 2021]