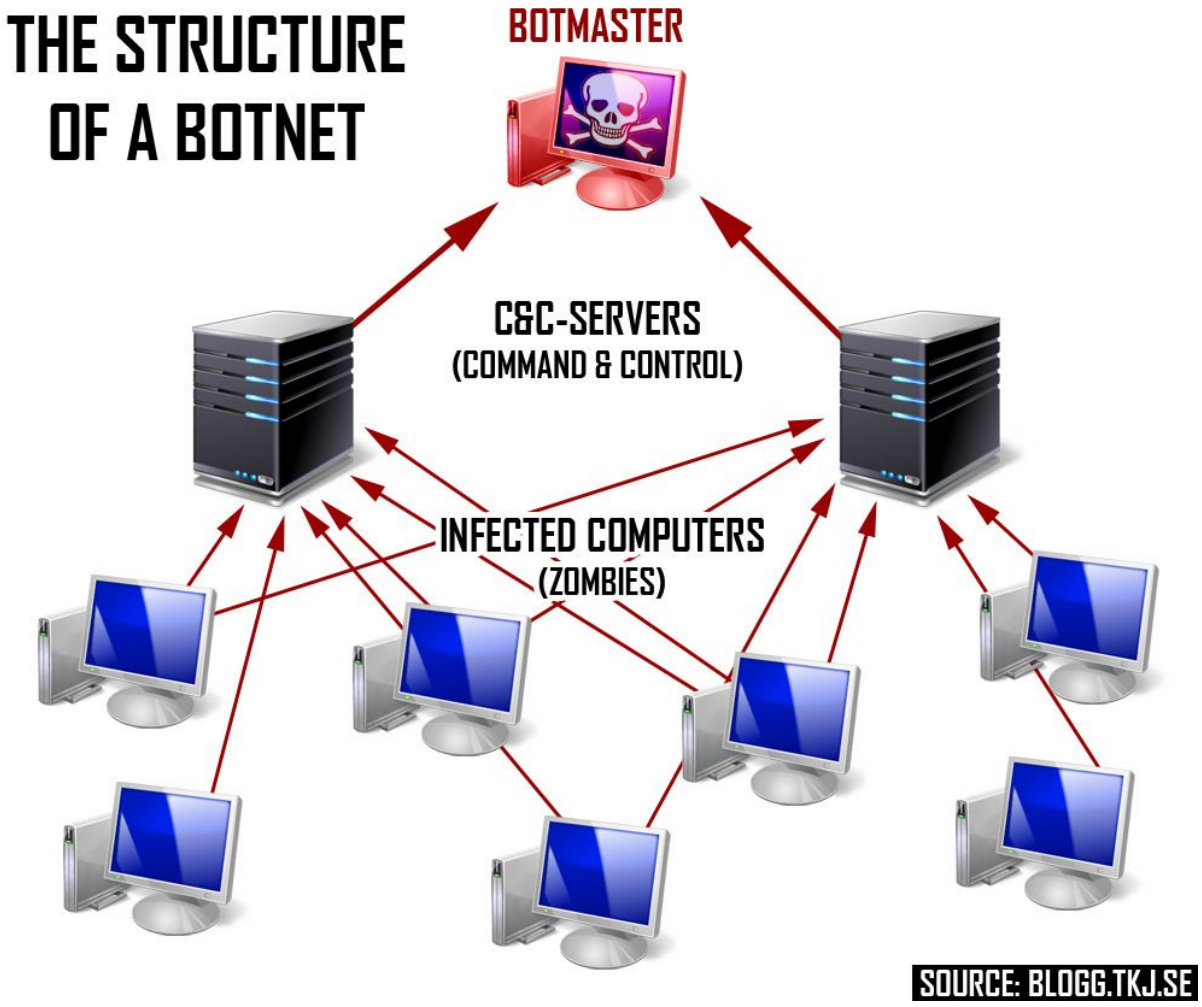
BOTNETS



Realizado por

Julio Antonio Fresneda García y Santiago Vidal Martínez

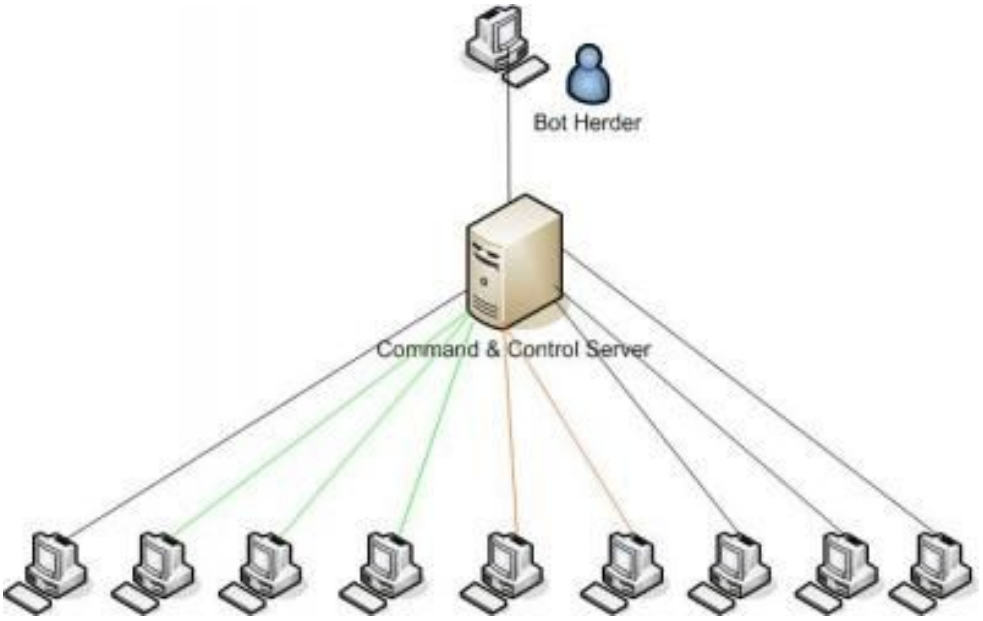
ÍNDICE

1. Introducción a los botnets

Sin duda, los botnets son en la actualidad una de las mayores amenazas de internet. Pero, ¿Qué son los botnets?.

Un botnet es un software robot que se ejecuta de manera autónoma.La finalidad de este software es controlar de forma remota cualquier máquina que forme parte de esta red de máquinas “zombies”.

Incluimos el siguiente gráfico para aclarar lo que es un botnet:



Partimos de que hay una persona (bot herder) que quiere controlar un grupo de máquinas y este distribuye un software y cuyo destino serán otras computadoras. Una vez accede el sistema software a la máquina, dicha máquina está a merced del bot herder.

El principal objetivo del bot herder podría ser la obtención de redes de banda ancha que siempre estén disponibles.

El hecho de que estén aumentando el número de máquinas de banda ancha, favorece a que se puedan comprometer (hacer que una máquina forme parte de una red zombi) más número de ordenadores.

Cuando detectan las máquinas, los atacantes acceden a la máquina y buscan sus vulnerabilidades. Ya conocido esto, se infecta con un bot que se comunica con otro bot. Este último es el bot que controla el resto de bots.

2. Funcionamiento del botnet

En este apartado se va a explicar cómo funciona un botnet, y cómo el atacante los controla.

Una vez identificada la máquina objetivo, el bot se transfiere a sí mismo a la máquina comprometida. El bot puede usar TFTP (Trivial File Transfer Protocol), FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol) o CSend (extensión de IRC).

Los bots se pueden propagar y controlar mediante IRC, HTTP o P2P.

Una vez se transfiere el bot a la máquina, éste procede a ejecutarse. Cuando se inicia, intenta conectarse a un servidor. Para ésto el bot usa un nombre dinámico DNS (que puede obtener de webs como dyndns.org) en vez de una IP codificada, ya que así el bot puede ser trasladado a otro host con relativa facilidad. Algunos bots incluso se eliminan a sí mismo bajo ciertas condiciones, como que el servidor dado sea localhost o estar en una subred privada, ya que son situaciones inusuales.

El bot intentará unirse a un canal maestro, normalmente con contraseña para mantener extraños fuera del canal.

El administrador de la red de bots debe autentificarse para tener control sobre estos bots. Esta autentificación se realiza, por ejemplo, con la ayuda de un comando y el prefijo “auth”, que se utiliza para la conexión del controlador con los bots.

Una vez que el administrador es autenticado, tiene total libertad de maniobra con los bots:
Puede buscar información importante en cualquier máquina comprometida, y el envío de ésta a otra máquina. Puede hacer DDoS a individuos u organizaciones, etc. Más adelante describiremos varios ejemplos.

En el el seguimiento de botnets (más conocido como “tracking botnets”) el bot debe comunicarse con el controlador para recibir instrucciones, enviar información, etc. Conectarse directamente al controlador es una mala idea, ya que podría poner en peligro su ubicación. En lugar de ello, se suele usar un proxy.

Sin embargo, podría ser mejor opción un enfoque más activo: IRC.

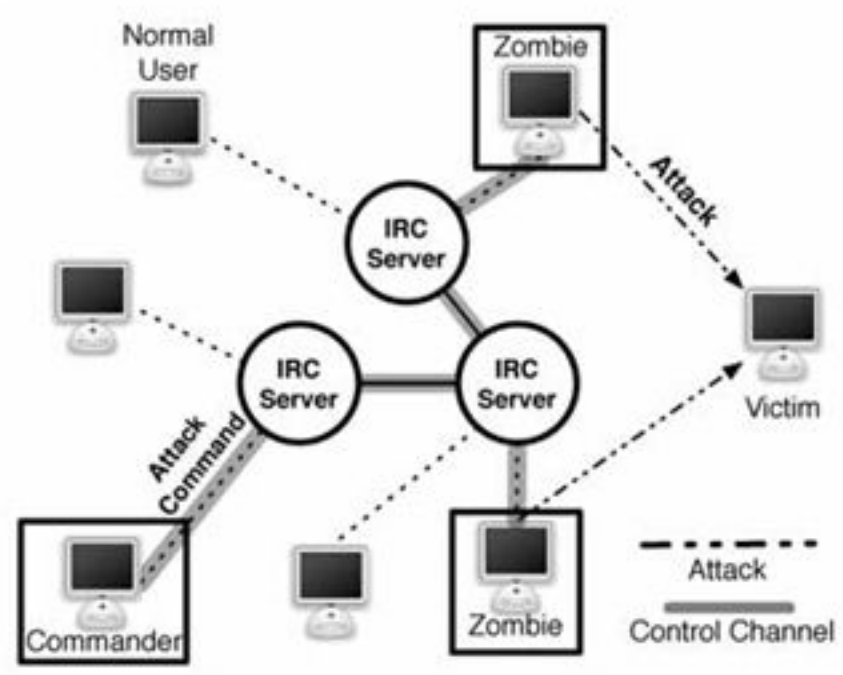
El IRC es un conocido punto de intercambio público que prácticamente permite la comunicación instantánea.

IRC tiene diversas ventajas:

Proporciona un protocolo común que se despliega ampliamente a través de internet. Tiene una interfaz simple y una sintaxis de instrucciones basada en texto. Hay un gran número de redes de IRC que pueden ser usadas como punto de intercambio públicos. Además, las redes de IRC facilitan el anonimato, ya que hay disponibles una serie de herramientas que lo facilitan, y la mayoría de redes carecen de autenticación fuerte.

De este modo, IRC ofrece, baja latencia, disponibilidad, y anonimato para lograr comunicación en la *botnet*.

Una red IRC se compone de uno o varios servidores. En una botnet clásica, cada bot se conecta a la red IRC o un servidor IRC oculto en otro sistema. El bot entonces entra en un canal para que pueda recibir directamente las instrucciones de un controlador.



Otro método que los atacantes utilizan para controlar un botnet es HTTP.

Mediante HTTP, el administrador configura un bot para acceder a un script PHP de algún sitio web, incluyendo toda la información e identificación en la URL.

Con este método, se puede crear una interfaz web para el seguimiento y control de la botnet. El administrador puede usar esta interfaz para enviar instrucciones a cualquier bot o a todos ellos, a través del protocolo HTTP.

Una forma de ocultar más el bot, es recibir sus instrucciones a través de una consulta en un sitio web bajo el control del administrador de la botnet. El bot tiene un algoritmo que obtiene la información

conveniente de esa consulta, aparentemente limpia, obteniendo las instrucciones necesarias.

Una vez infectado, el sistema zombie intenta conectarse al servidor web, para así comunicarle la IP de la máquina, el número de puerto y la cadena de identificación. Esta información es utilizada para identificar y comunicarse con bots específicos.

Algunos ejemplos de instrucciones para los bots son:

- Descargar y ejecutar archivos desde una URL
- Ejecutar comandos *shell*
- Ajustar la ubicación de almacenamiento de registros URL
- Ajustar el archivo de hosts en la máquina

Además de mediante redes IRC y HTTP, el bot puede usar P2P para expandirse.
Su principal característica es que no tiene ningún servidor central, por lo que no puede ser apagado para desactivar la botnet.

En una botnet P2P, los bots que pueden recibir conexiones entrantes actúan como servidores (llamados supernodos) y aquellos que no pueden simplemente realizar tareas desde el botmaster (conocidos como trabajadores). Los supernodos se conectan a otros supernodos y pasan mensajes entre ellos para mantener la red sincronizada y los trabajadores se conectan a múltiples supernodos para recuperar comandos. Para que los trabajadores mantengan una lista actualizada de supernodos, cada uno de ellos responde a un comando de solicitud con una lista de direcciones IP para otros supernodos que conoce (esta lista varía en tamaño dependiendo de botnets; por ejemplo, Kelihos envía 500 IPs y ZeroAccess2+ solo envía 16). Los trabajadores descargan listas de múltiples supernodos y los almacenan localmente

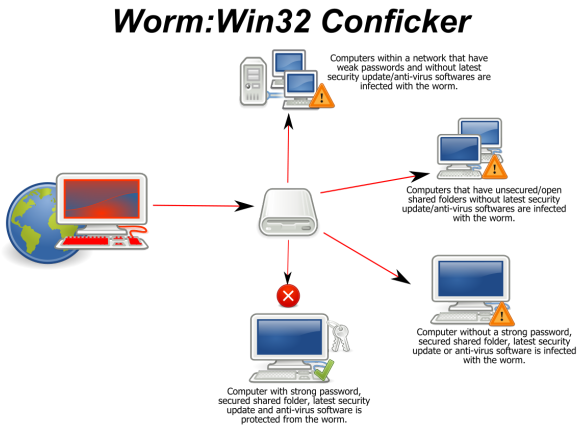
para garantizar que puedan mantener la conectividad con el botnet, incluso con un mapa de supernodos en constante cambio.

3. Ejemplos de botnets

Hay múltiples redes zombi, entre las cuales vamos a destacar las cinco redes siguientes:

1. Conficker

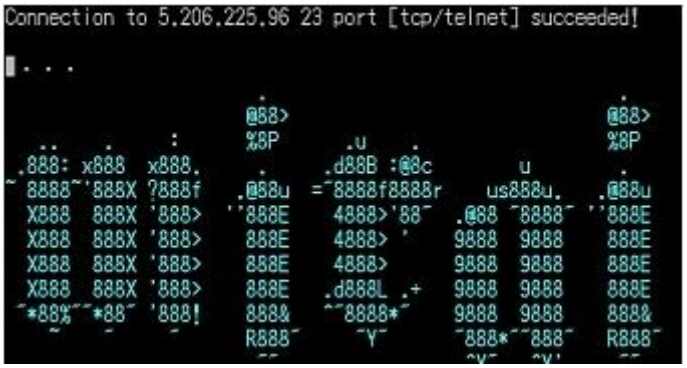
Conficker es un malware de tipo gusano que afecta principalmente a Windows. Principalmente se suele utilizar para robar información o para realizar spam. También es conocido como Downup, Downandup o Kido.



Este malware se propaga a través de la vulnerabilidad en el servicio Windows Server o a través de unidades extraibles o USB.

2. Mirai

Los objetivos de este malware son los routers, grabadoras digitales de vídeo y cámaras de vigilancia.



Se ha utilizado para realizar ataques DDoS (denegación de servicio). Además los sistemas afectados son Windows y dispositivos con sistemas embebidos Linux. Principalmente se infecta mediante el uso de credenciales.

3. AndroidBauts

Es un malware de tipo troyano que afecta principalmente a sistemas operativos Android. La función de este malware es mostrar anuncios en el dispositivo, recoger y enviar datos como el IMEI, la localización del GPS, etc.

El principal método de infección es mediante las aplicaciones existentes en el Google Play Store, sin embargo, estas aplicaciones son retiradas inmediatamente.

4. Necurs

Nercurs es un troyano que infecta ordenadores con Windows como sistema operativo. Los ordenadores infectados pasan a ser parte de la botnet. Su principal objetivo es el robo de información bancaria o la distribución de ransomware.
Su principal método de infección es drive-by-download, es decir, el malware es descargado de internet (automáticamente o accidentalmente), como por ejemplo gracias al spam.

5. Nivdort

Nivdort es un malware de tipo troyano que afecta principalmente a Windows. Sus funciones son obtener información como las teclas que

se han pulsado, el listado de aplicaciones abiertas, el historial de los navegadores, información sobre tarjetas de crédito y usuarios y contraseñas.

El método de infección principal es a través de correos electrónicos con archivos adjuntos (archivos que son maliciosos).

4. Seguridad ante ataques DDoS y botnets

Proteger una computadora frente a un botnet no es tan sencillo como parece. Principalmente hay que evitar que te introduzcan en una botnet. Para conseguir esto es necesario tener un buen antivirus y desconfiar de todo lo que nos llega de internet.

Ver si somos un objetivo de una botnet es más sencillo para aquellos usuarios que tienen el ancho de banda limitado. Además para descubrir si el equipo está infectado, hay herramientas anti-malware.

Para usuarios con conocimiento se puede utilizar una herramienta de diagnóstico como ESET SysInspector o incluso observar los procesos que corren en el sistema o los programas instalados.

También hay que tener en cuenta que en cualquier momento nos pueden realizar un ataque de denegación de servicio. Es por esto que debemos defendernos de esto y cuanto más cercana sea la defensa a su origen, mejor.

Ante un ataque hay que tener en cuenta cómo impactaría la pérdida de internet. Tenemos que realizar una monitorización periódicamente de forma que se detecte de forma temprana.

Ante el ataque DDoS, hay que mitigar los efectos de este, además hay que avisar a los organismos pertinentes para que intenten desarticular a este tipo de redes.

Cabe destacar que es muy probable que alguno de nosotros seamos el objetivo de un ataque de DDoS. Sin embargo, tener un plan de contingencia puede solucionar esta situación.

Vamos a mostrar un sencillo proceso para detectar si somos parte de una botnet que ya haya sido detectada:

- Accedemos a https://www.osi.es/es/servicio-antibotnet
- Pulsamos en la imagen que pone chequea tu conexión
- Aceptamos las condiciones de uso
- Pulsamos en chequear mi conexión

Una vez realizado esto mostrará un mensaje indicando si la ip está relacionada con incidentes de la botnet.

No obstante a pesar de esto, el sistema no es fiable al 100% por lo que no hay que fiarse completamente de esto.

Además aquí podemos observar la recomendación del sistema: "Te recomendamos que ejecutes periódicamente este servicio mediante la instalación de nuestro plugin de chequeo."

5. Bibliografía

https://www.osi.es/es/servicio-antibotnet/info/conficker
http://culturacion.com/que-son-las-botnets/
https://www.welivesecurity.com/la-es/2014/10/29/top-5-botnets-zombi/

https://www.welivesecurity.com/media_files/white-papers/Passing_Storm.pdf
http://www.criptored.upm.es/guiateoria/gt_m142f1.htm
https://www.osi.es/es/servicio-antibotnet/info/mirai
https://www.osi.es/es/servicio-antibotnet/info/androidbauts
https://www.osi.es/es/servicio-antibotnet/info/necurs
https://www.osi.es/es/servicio-antibotnet/info/nivdort
https://www.hazhistoria.net/blog/botnets-las-redes-zombis-de-ordenadores
https://www.pabloyglesias.com/mundohacker-botnets-y-ataques-ddos/
https://www.welivesecurity.com/la-es/2014/10/27/botnets-como-combatirlas/
https://www.youtube.com/watch?v=qje_OHbGvH4
https://www.malwaretech.com/2016/01/exploring-peer-to-peer-botnets.html