Manual de Usuario

Condiciones iniciales.

Para el correcto funcionamiento de IRCBot y BotAdmin es necesario que todos los equipos tengan instalado Java Runtime Enviroment versión 6 o posterior.

Uso

Existen dos formas de manipular a los bots:

[1] Linea de comandos:

En esta manera es necesario tener un cliente IRC instalado, después es necesario conectarse a:

Servidor: irc.freenode.net
Canal: #pruebastareac2016 Nick:
definido por el usuario.
Puerto: 6667

Para hacer el análisis de manera local:

Agregamos la dirección 192.168.1.30 irc.freenode.net al archivo host de windows.
Iniciamos el servidor irc y un cliente (como pidgin) en Debian.
De esta manera,podemos hacer las cosas localmente.
Una vez configurado (si se quiere hacer localmente), podemos enviar a los bots

Instrucciones:

Una instrucción tiene el siguiente formato:

<<nicknamebot>>!@{command} {param1} {param2} {param3}

donde:

El nickname {idOS}_{IdMaquina}_{Num} compuesto por:

IdOS es el identificador del sistema operativo.
IdMaquina es el identificador particular del bot tomado de alguna característica de Software o Hardware.
Numero: un numero aleatorio.

Por ejemplo:
Una maquina con windows 7 tendría un identificador parecido a

W_7cee21b7_23.

!@: Es el prefijo para todas las instrucciones.

{command}:

Es el identificador de los comandos: cifraByteRot,cifraBinDes,etc.
donde:

Param1,param2,param3: son argumentos para el comando p1 :=
ruta absoluta del archivo sobre el que se realizara el comando P2:=
rotación o clave para hacer xor o clave des.
P3:= clave xor, si se ejecuta cifraByteRotXOR, en este caso p2
seria la rotación.

Entonces, para pedirle al bot W_XP287686_48 que cifre el archivo claves.txt con cifraByteRot utilizamos la siguiente instrucción:

<< W_XP287686_48>>!@cifraByteRot “C:\Documents and Settings\nuevoAdmin\Escritorio\prueba.txt 4”

Observe que hay un espacio entre el comando y la ruta del archivo, y un espacio entre la ruta y el parámetro de rotación.

Ademas que si la ruta del archivo tiene espacios debemos encerrarla entre comillas.

Si queremos que todos los bots ejecuten una instrucción simplemente omitimos el operador nick.

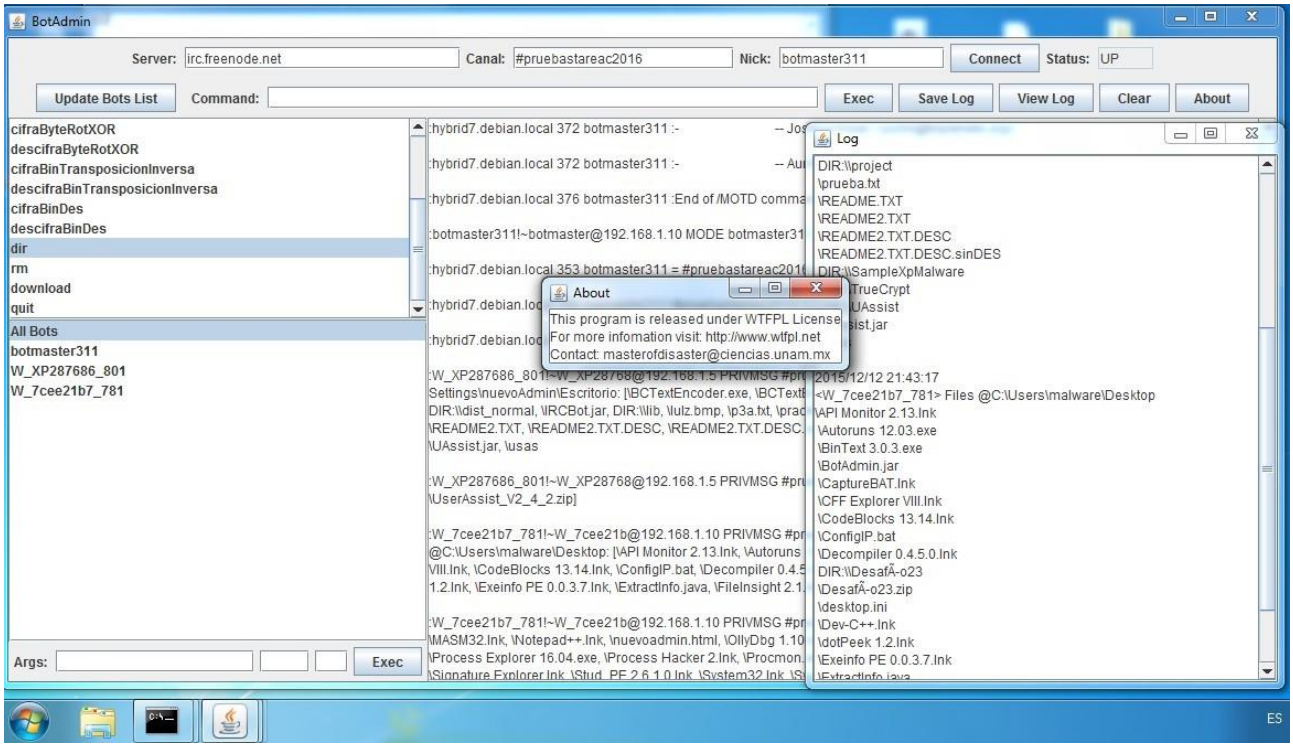
Por ejemplo; para listar el directorio desde el cual se esta ejecutando IRCBot hacemos:

!@dir

Note que hay un espacio después de la r sin este espacio los bots devolverán un resultado vacío.

[2] Interfaz Gráfica

Proporciona un medio mas intuitivo para interactuar con los Bots, sin perder funcionalidad alguna del método [1].



BotAdmin en W7

La interfaz se distribuye en un .jar no vinculado con IRCBot, este contiene un cliente IRC modificado.
Inicialmente BotAdmin se conecta:

Servidor: irc.freenode.net
Nick: botmaster+un numero aleatorio menor a 513 ej botmaster123
Canal: #pruebastareac2016 Puerto: 6667

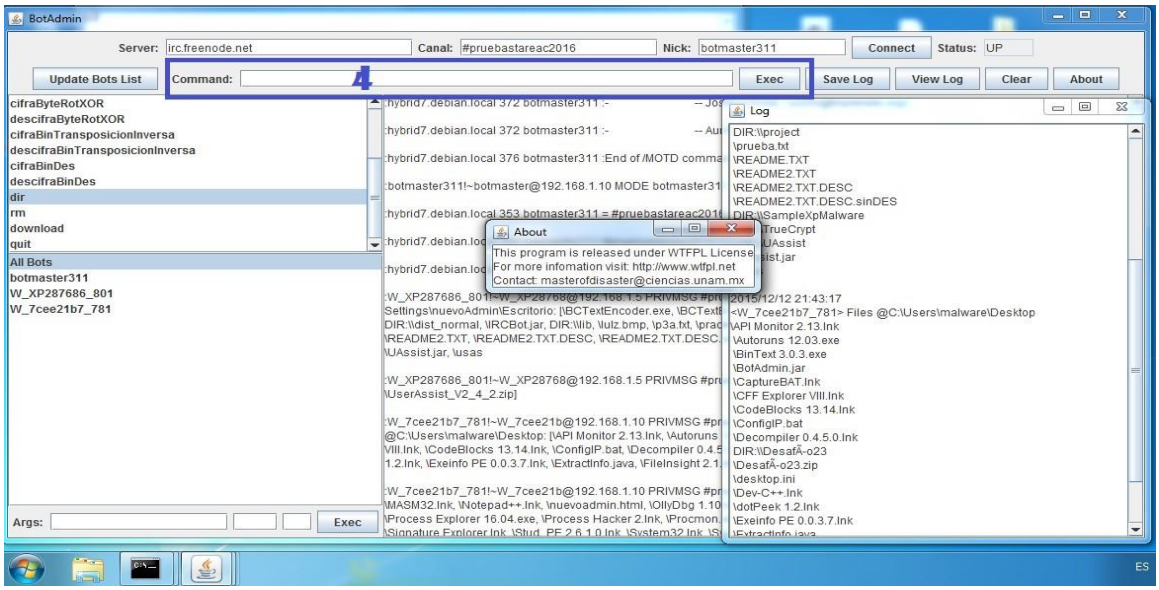
Estos parámetros pueden cambiarse si se ejecuta el jar desde una terminal.
Java -jar {nick} {server} {channel} {puerto}.
Donde el canal se ingresa sin #.

Ademas, la interfaz provee una funcionalidad adicional, mantiene un registro de los archivos cifrados y la información obtenida de los bots.

Dando Instrucciones:

Para dar instrucciones a los bots mediante la interfaz gráfica existen 2 opciones:
Opción 1):

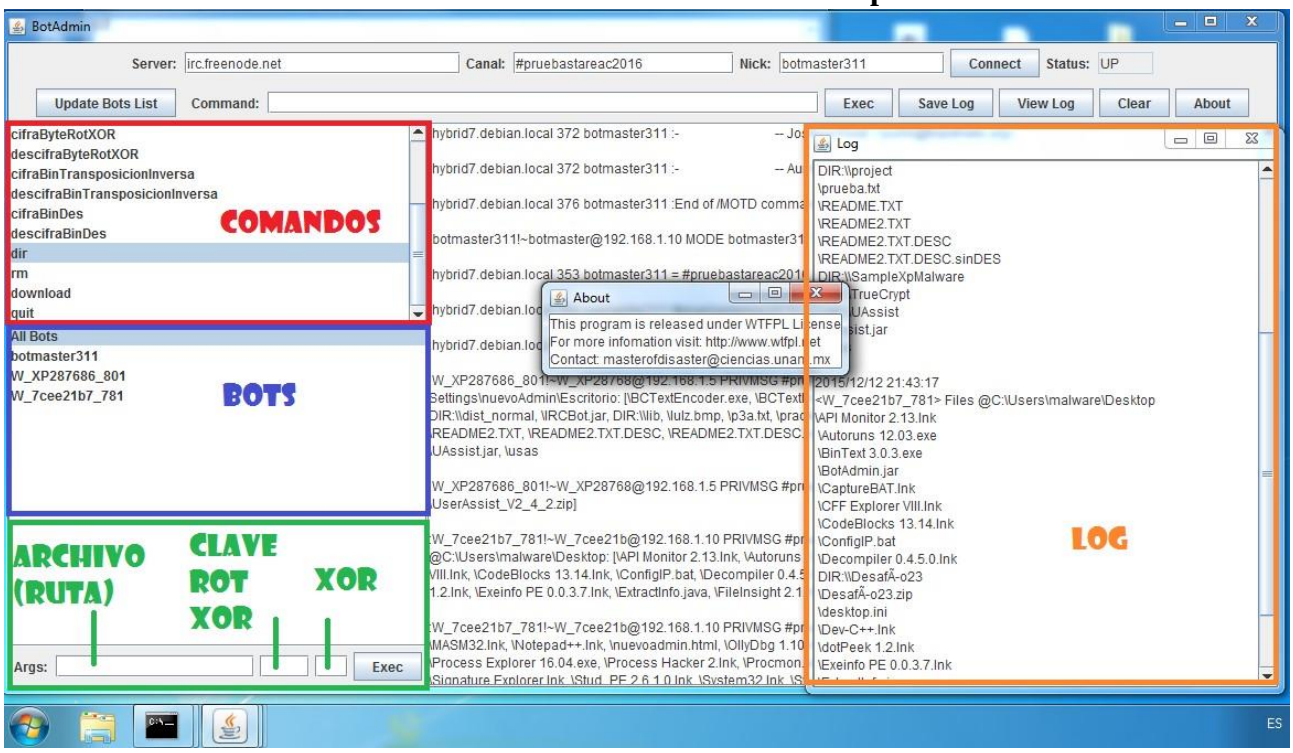
Dar un comando especifico como se hace en el método del cliente irc, es decir dando la instrucción completa:
Para esto, escribir el comando en la barra de la sección 4 y dar clic al botón exec.



Opción 2):

Esta es la forma mas intuitiva:

Primero actualizar la lista de bots dando click en el **boton UpdateBots.**



Seleccionar el comando a ejecutar de la lista de opciones disponibles:

Seleccionar el bot que realizara el comando, si se quiere que sean todos seleccionar All Bots: Rellenar los parámetros en la cajas:

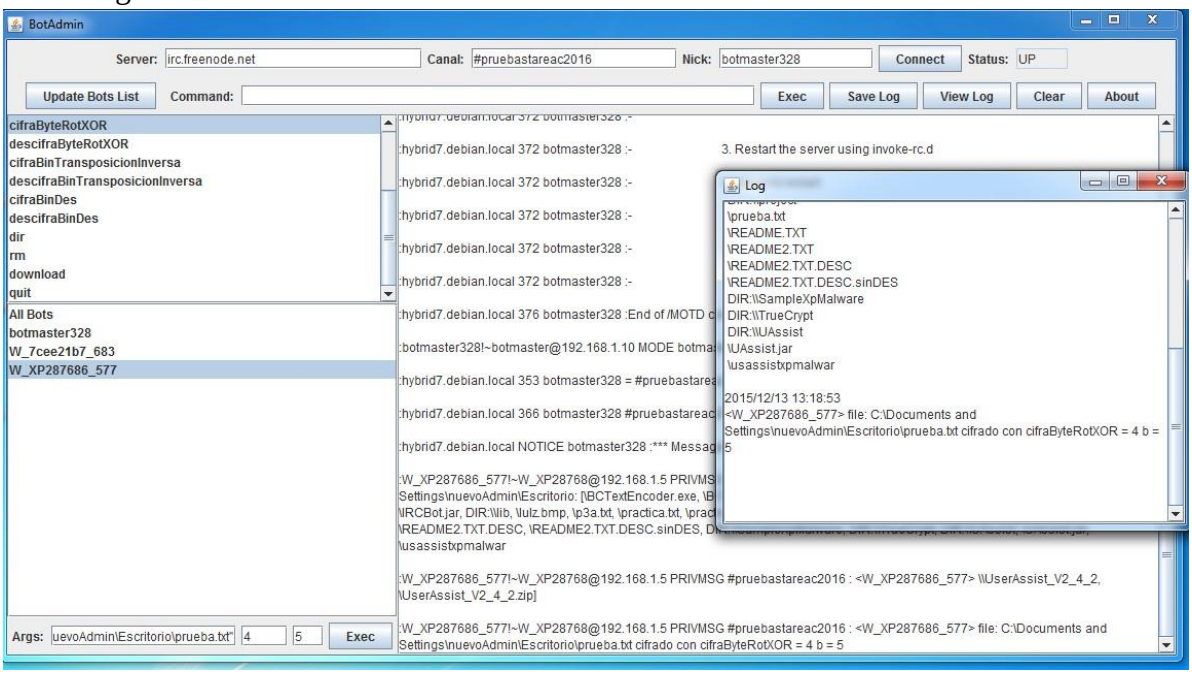
Donde:

El primer parámetro es la ruta del archivo sobre el que se ejecutara el comando.

El segundo parámetro es el primer argumento para el comando.

El tercer parámetro es el segundo argumento para el comando.

Por ejemplo:
Si queremos que el bot W_XP287686_577 cifre el archivo prueba.txt localizado en su escritorio con el método cifraByteRotXOR con una rotación de 4 bytes y XOR con 5 la configuración sería:



Por ultimo para enviar la instrucción damos clic al botón Exec adyacente a la caja de argumentos.
Al hacer clic en el botón View Log es posible ver que se registro el cifrado de este archivo con sus parámetros.
Ademas del bot que genero la acción: esto representa una ventaja ya que si se pierde la conexión con este bot el identificador único en su nickname nos servirá para identificarlo después.

Notas Importantes:

[0]
En esta versión, la función de seleccionar al bot que ejecutara la acción ha sido implementada.

[1]
La interfaz gráfica no lista en la sección 3 todos los comandos que pueden ejecutarse sobre el bot. Es decir, solo muestra los directamente implementados, sin embargo es posible llamar comandos nativos del sistema.

Por ejemplo:
Si hacemos !@mspaint (con un espacio al final), todos los bots que estén corriendo bajo algún sistema operativo Windows abrirán una ventana de Paint.

[2]
BotAdmin solo muestra en la lista de bots aquellos que se encuentran conectados usando el jar IRCBot.jar
Es decir, si alguien se conecta usando un cliente propio no aparecerá en esta lista, a menos que se conecte después del BotMaster.
La razón es que el cliente IRC de BotAdmin.jar agrega los clientes cuando estos responden al ping con “I got pinged” o cuando alguien entra después de iniciar BotAdmin.jar

[3]
Utilizar BotAdmin.jar para manejar la botnet es la manera mas segura de hacerlo, ya que el cliente IRC de este jar no tiene habilitada la opción de ejecutar comandos externos.

[4]
El panel superior de conexión aun no esta implementado.