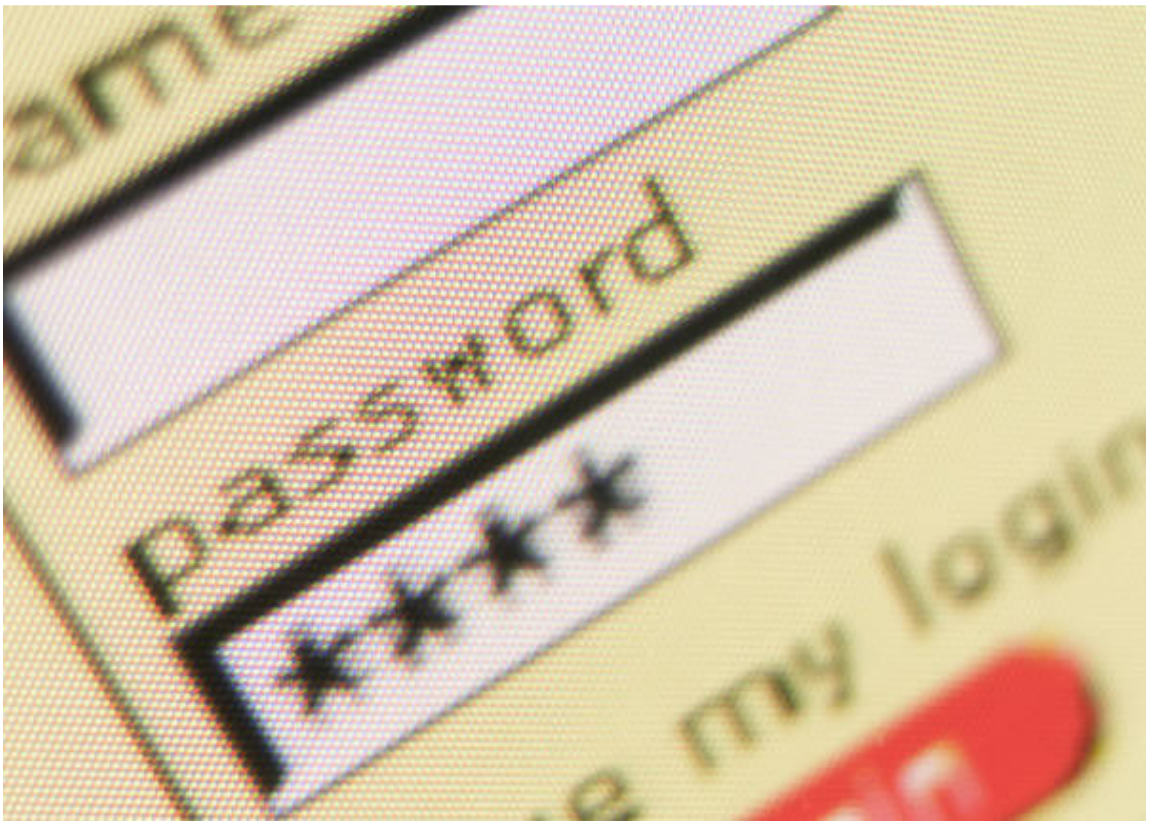
M-ZINE IV

Malware Magazine #4



Tema: **Stealers**

ANTRAX

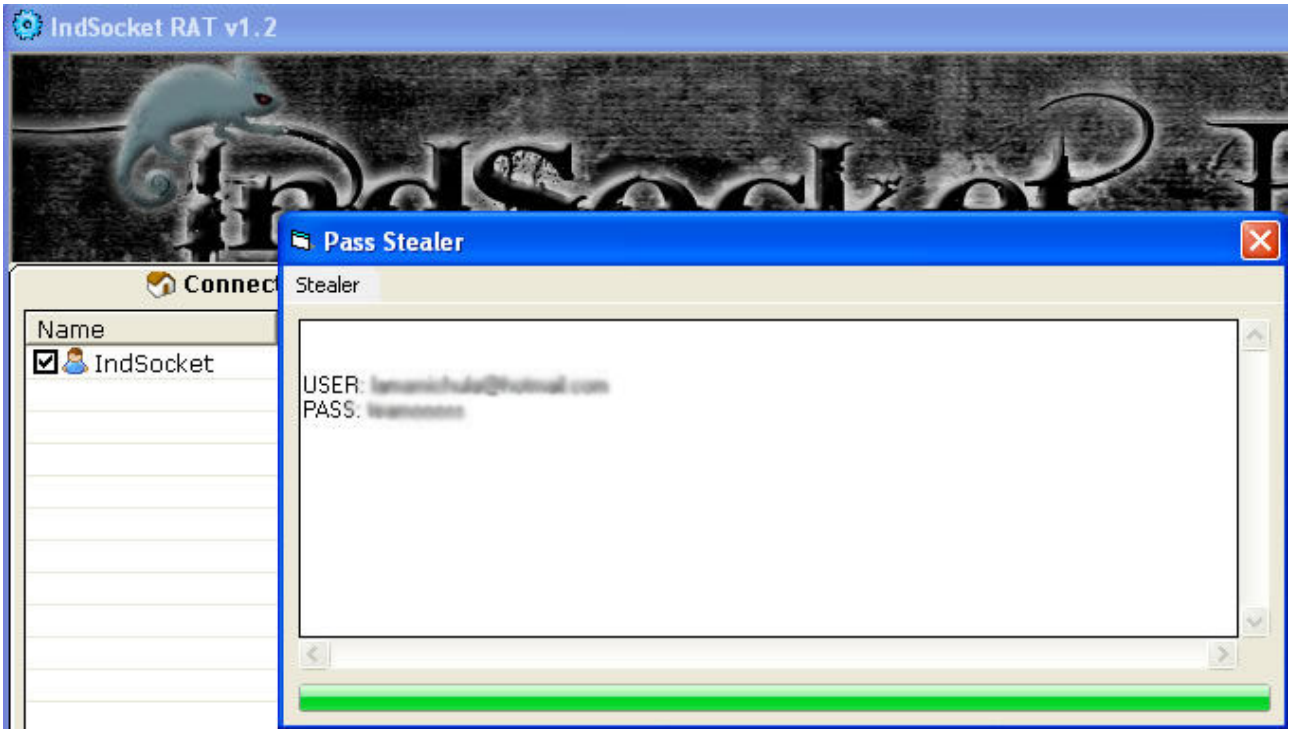
www.antrax-labs.net

¿Qué es y para qué sirve un Stealer?

Un stealer es un malware encargado de capturar y mostrar todos los logins almacenados en una PC.

La mayoría de los troyanos, tienen la opción de mostrar las contraseñas almacenadas, pero a lo largo de este tutorial, les mostrare las diferencias que hay entre capturarlas con un troyano y un stealer.

En la siguiente imagen les mostrare una captura de este excelente troyano que es el IndSocket RAT que trae incorporado la opción de mostrar los logins almacenados.

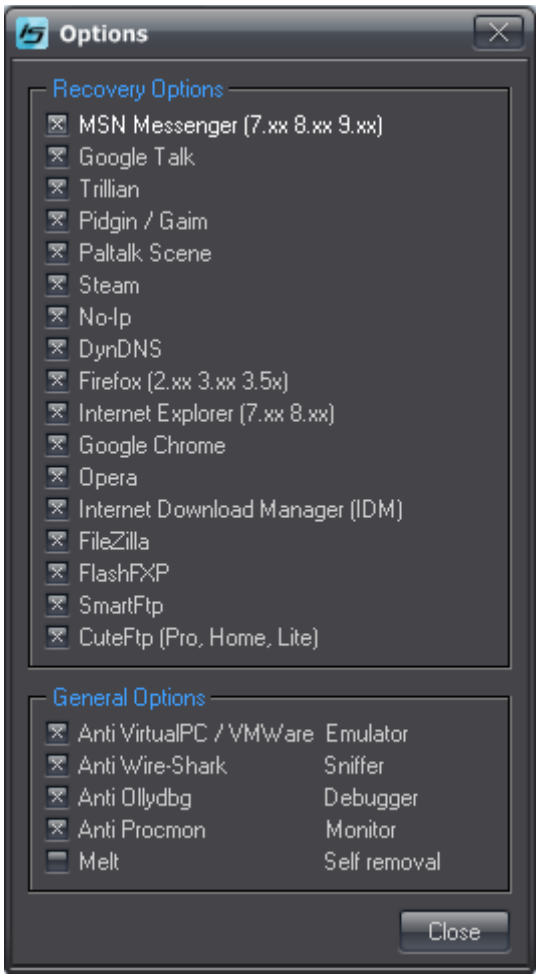


Como se puede ver, aparece el user y pass de un mail.

Entonces… Para que están los stealers, si con un troyano también podemos ver los logins…

La respuesta es simple, un troyano solo muestra las Pass de un solo remoto que nosotros seleccionemos, en cambio el stealer a demás de capturar logins de todo tipo, son mas ordenados. A demás de esto, los Stealers son mucho más completos, ya que capturan distintos tipos de pass de varias aplicaciones. El que les enseñare hoy día, captura una gran cantidad de pass. Los troyanos por lo general capturan pass de MSN, IE, Firefox

entre otros. En cambio el que utilizaremos captura cantidad más notable que los troyanos:



Esto se debe a que los stealers solo están diseñados para sacar logins.

En esta entrega, les enseñare a montar un stealer que trabaja con base de datos SQL y que almacena, guarda y muestra de forma ordenada todos los logins capturados.

Antes de comenzar, quiero aclarar que no me hago responsable por el mal uso que se le pueda dar a esto.

Este material es expuesto para aprender el funcionamiento de un stealer. Lo que ustedes hagan con él, ya será bajo su responsabilidad.

PARTE I

Lo que necesitaremos será un hosting con Cpanel y el Stealer. En esta entrega utilizare el iStealer.

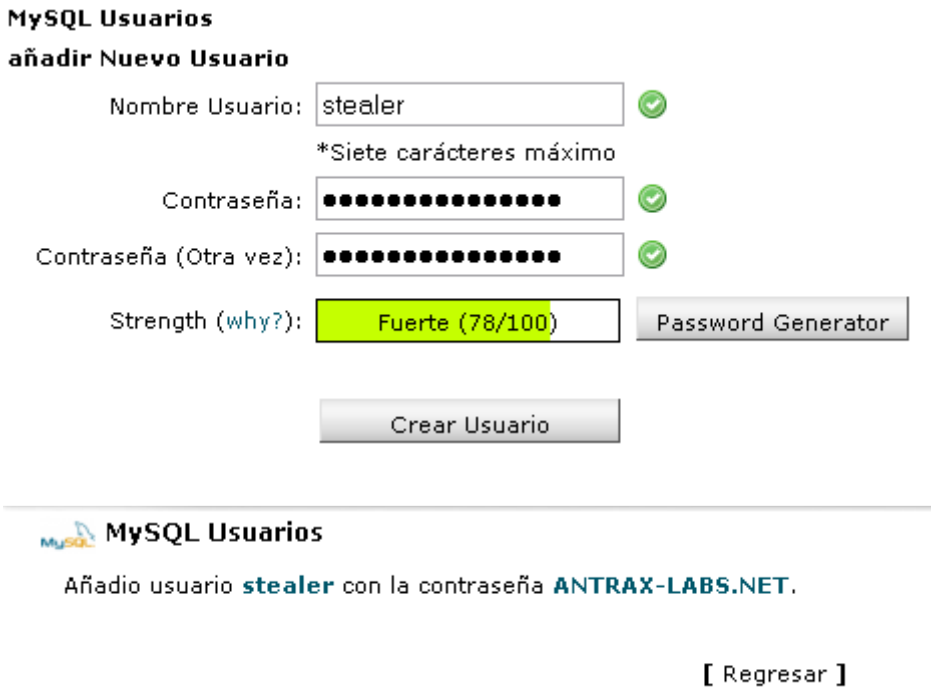
Si el hosting es gratuito corremos el riesgo de que lo den de baja y perder todo.

Yo utilizare uno prestado, que será solo para testear el stealer y mostrarles su funcionamiento.

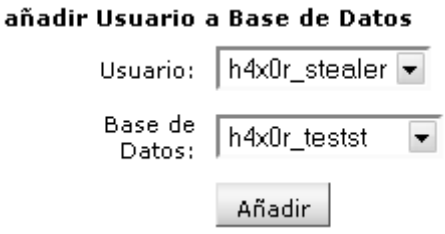
Vamos a nuestro Cpanel y crearemos una base de datos

Bueno, ahí ya quedo nuestra base de datos creada.

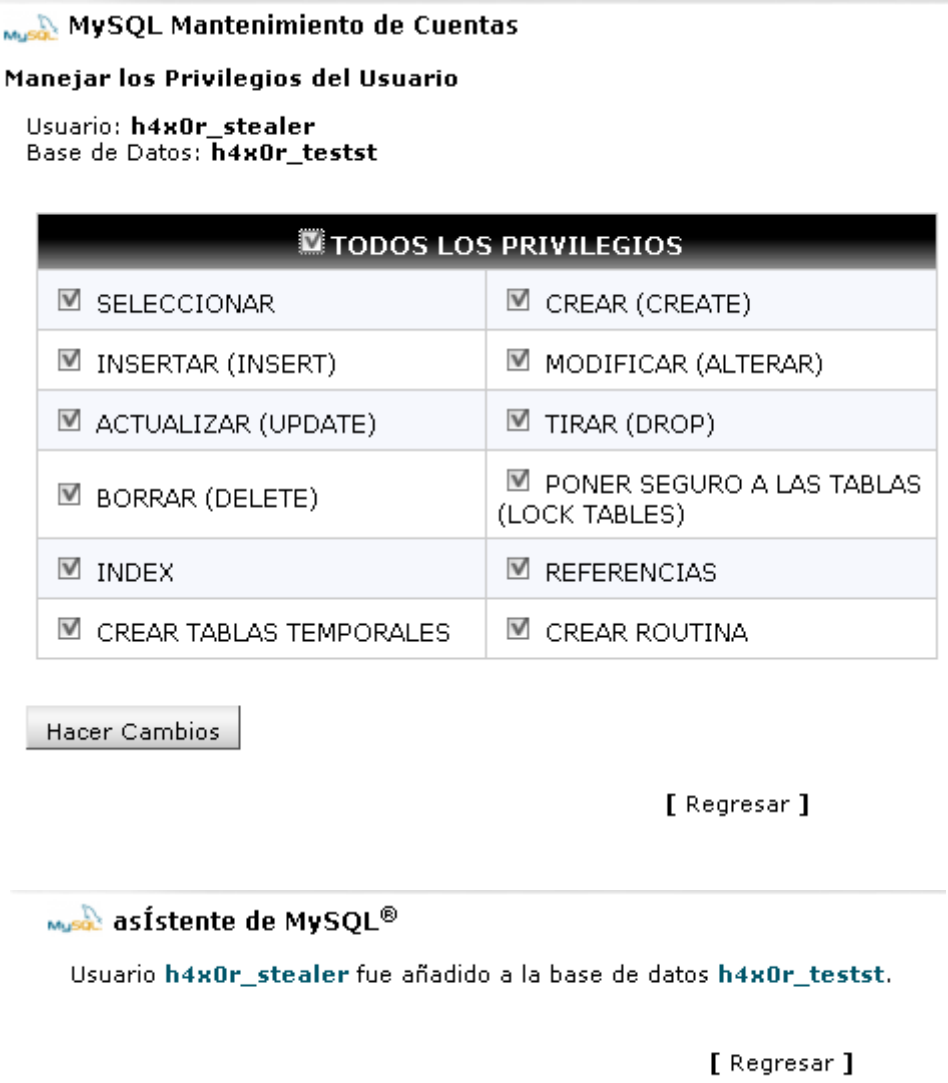
Ahora lo que debemos hacer es crear un usuario para añadirlo a la base de datos



Bien, lo que sigue es vincular a ese usuario con la base de datos.



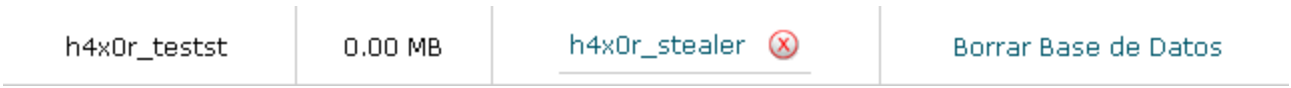
Ahora le aplicamos los permisos



Y listo!

Debemos recordar los datos de la base de datos, el usuario y la contraseña para poder configurar el Stealer.

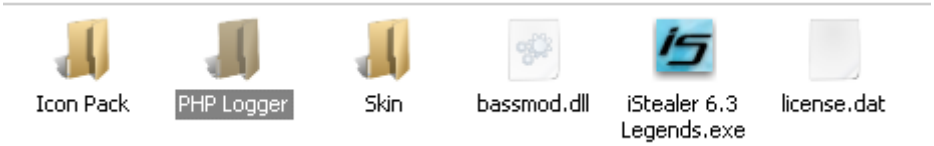
Aca vemos como quedo finalizado:



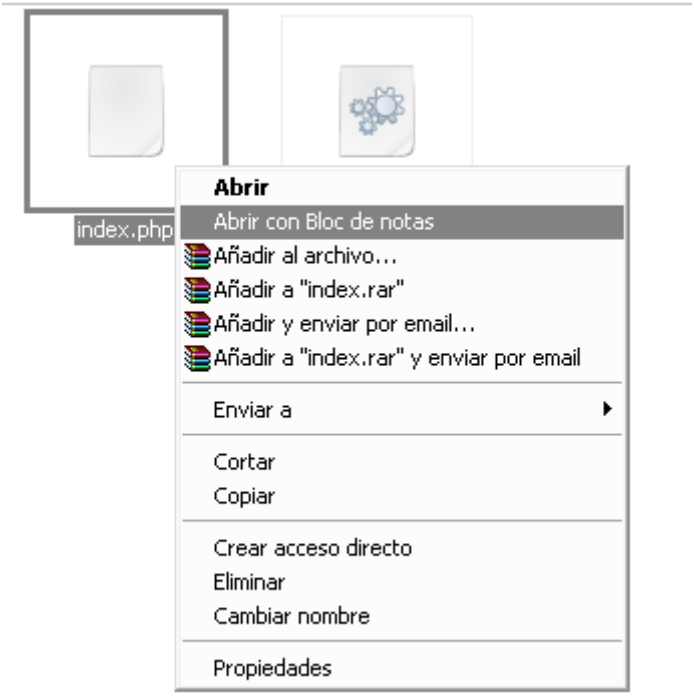
Como se puede ver, ahí esta la bd con el usuario vinculado

PARTE II

Lo que sigue es configurar el Stealer. Para ello vamos al directorio PHP Logger



Con algun editor de textos editamos el Index.php



Ahora podremos ver el código

```php
<?php
    // CONFIGURATION ********************************************

    $dbHost     = "127.0.0.1";       // MySQL host
    $dbUser     = "";    // MySQL username
    $dbPass     = "";    // MySQL password
    $dbDatabase = "";    // MySQL database name

    $username   = "admin";       // Login Username
    $password   = "admin";       // Login Password

    $logspage   = 50;            // Number of logs per page

    // **********************************************************
```

Reemplazamos por los datos nuestros

Comenzaremos desde la línea 4:

```
$dbHost     = "127.0.0.1";        // MySQL host
```

Modificamos y debe quedar asi:

```
$dbHost     = "localhost";        // MySQL host
```

Sigamos ahora a la siguiente línea, la 5 en donde deberemos colocar el usuario que creamos:

```
$dbUser     = "";   // MySQL username
```

Modificamos y debe quedar asi:

```
$dbUser     = "h4x0r_stealer";    // MySQL username
```

Pasamos a la línea 6, que debemos colocar la Contraseña que le asignamos a dicho usuario:

```
$dbPass     = "";   // MySQL password
```

Modificamos y ponemos la pass

```
$dbPass     = "ANTRAX-LABS.NET";  // MySQL password
```

Vamos a la línea 7, en donde colocaremos el nombre de la base de datos que creamos:

```
$dbDatabase = "";   // MySQL database name
```

Debe quedar asi:

```
$dbDatabase = "h4x0r_testst";// MySQL database name
```

Pasamos a la Linea 9, ya que la 8 esta vacia:

```
$username   = "admin";        // Login Username
```

La modificamos, por el usuario que nosotros queramos:

```
$username   = "ANTRAX";       // Login Username
```

Lo mismo hacemos en la línea 10, modificamos por una pass que queramos:

```
$password   = "root";         // Login Password
```

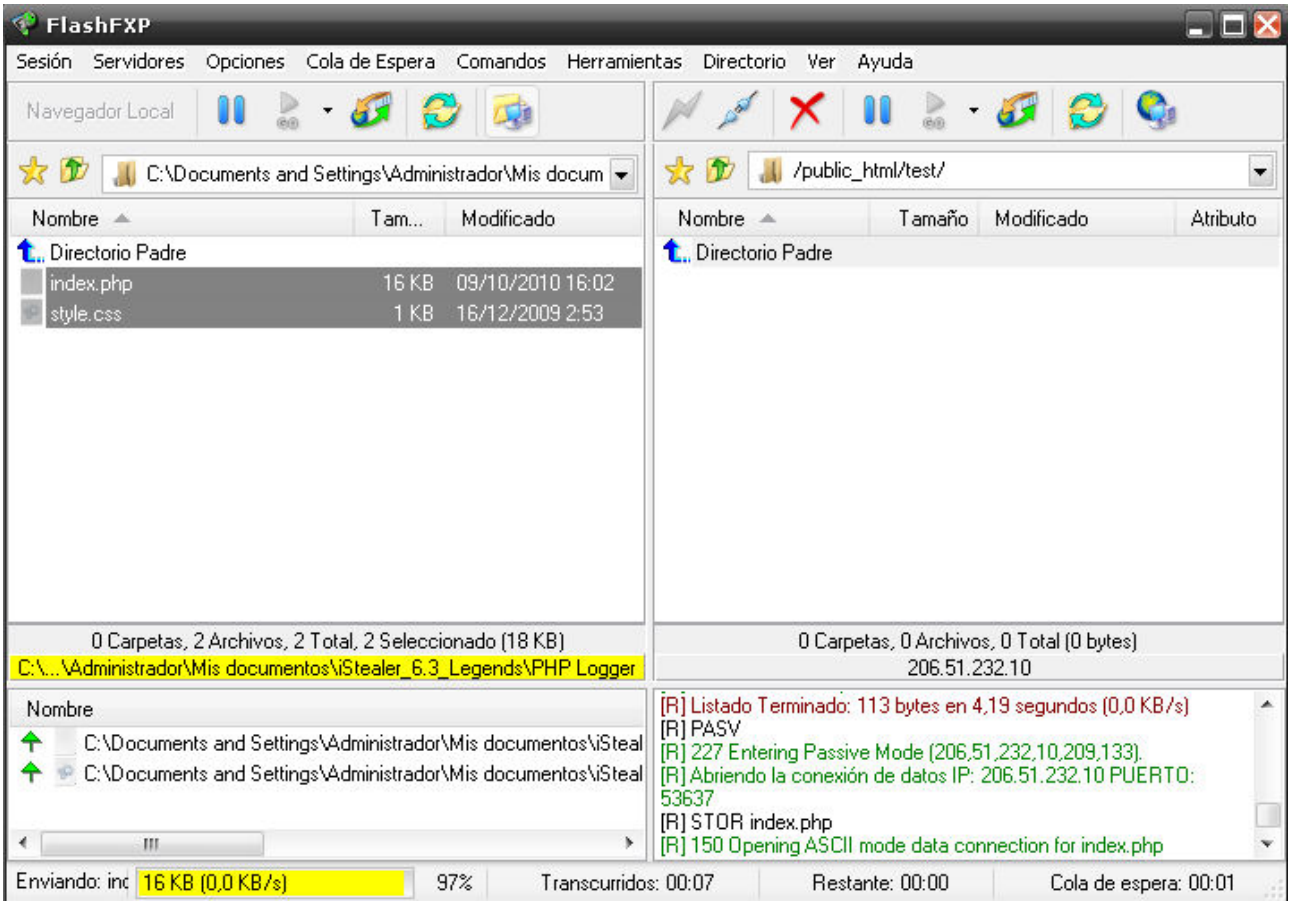
Aca les muestro una Captura de cómo quedo el mio terminado:

```php
<?php
    // CONFIGURATION ********************************************

    $dbHost     = "localhost";       // MySQL host
    $dbUser     = "h4x0r_stealer";   // MySQL username
    $dbPass     = "ANTRAX-LABS.NET"; // MySQL password
    $dbDatabase = "h4x0r_testst";    // MySQL database name

    $username   = "ANTRAX";      // Login Username
    $password   = "root";        // Login Password

    $logspage   = 50;            // Number of logs per page

    // **********************************************************
```

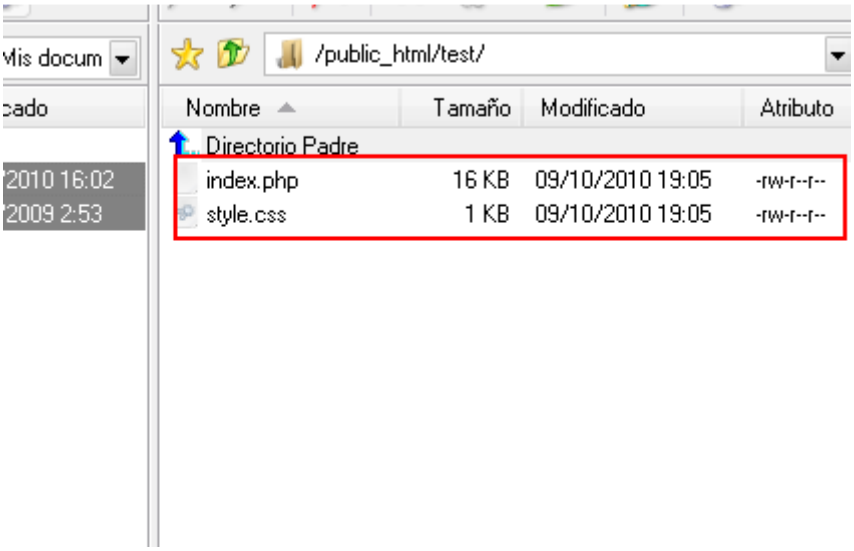
Guardamos y listo!

PARTE III

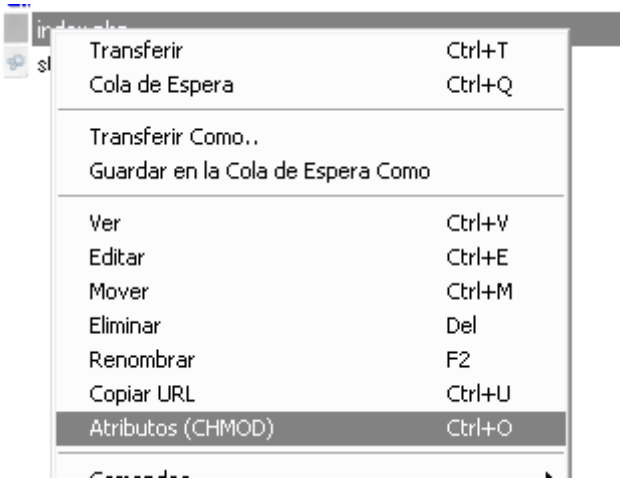
Lo que sigue es subir el index.php y la hoja de estilo por FTP a nuestro hosting.

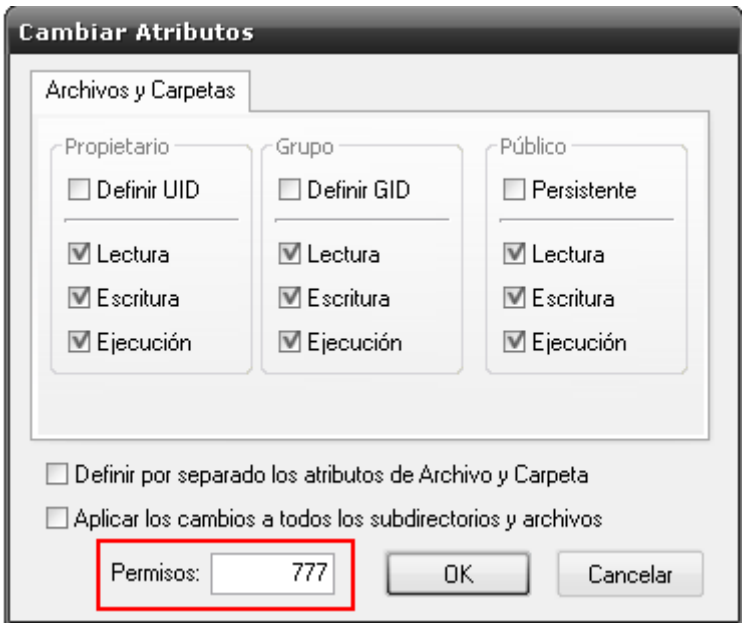


Una vez que subió todo

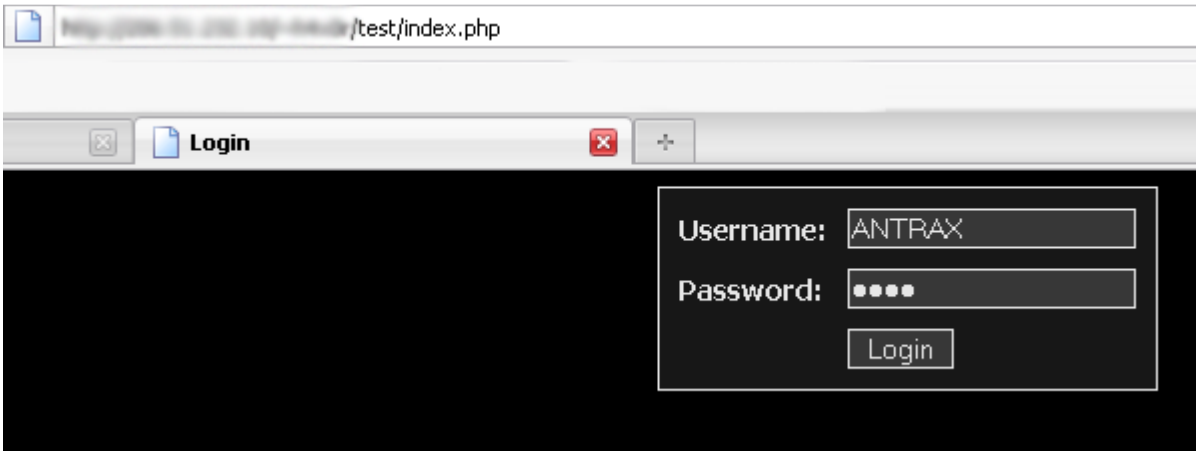


Para evitar futuros inconvenientes, le daremos permisos 777 al index.php

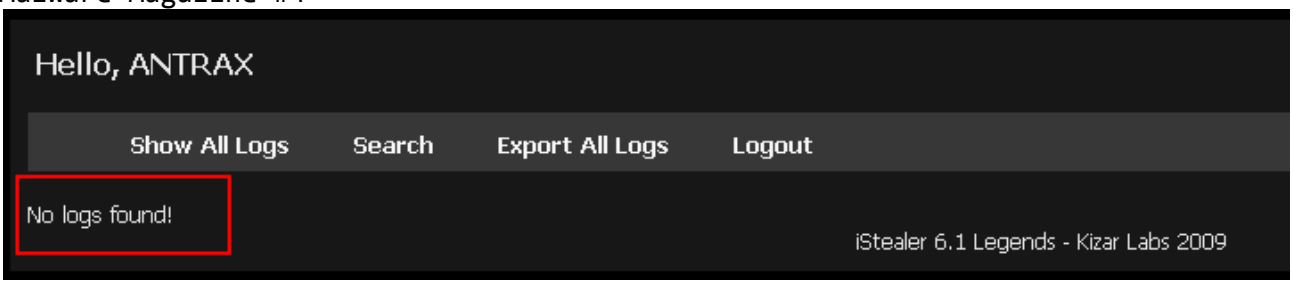




Ahora Entramos por la URL vía web y debería verse así:



Ingresamos al panel:



Si dice “No logs found!” quiere decir que hasta acá venimos todo perfecto.

De lo contrario mostrara errores en las tablas de base de datos o algún error de tipeo y deberemos revisar todos los datos que introducimos en el index.php

PARTE IV

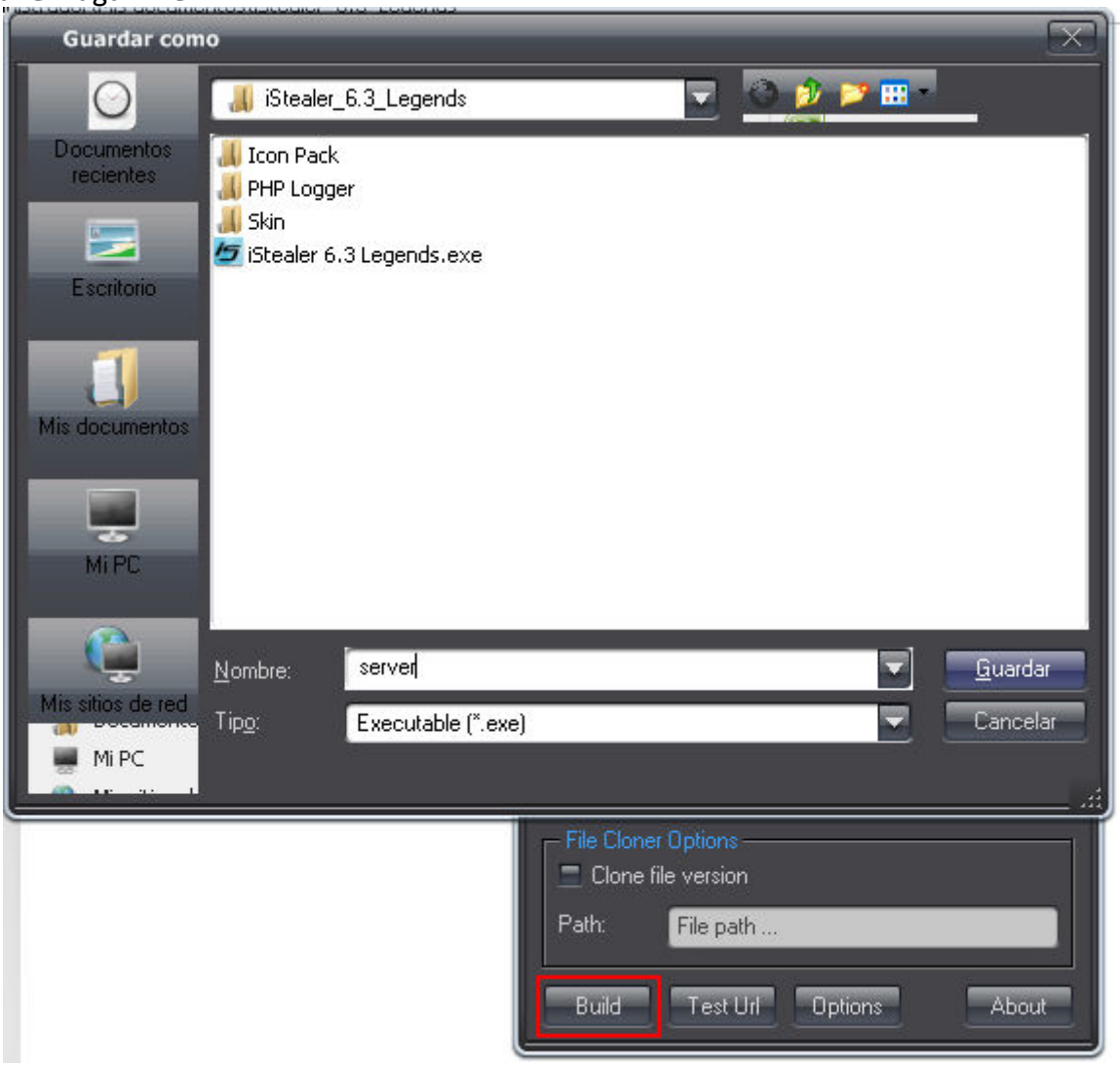
Bueno, casi llegando al final, lo que nos queda es crear el Server del Stealer.

Abrimos el Builder del iStealer

Colocamos la URL de donde tenemos el index.php y presionamos en el botón Test URL

Si es correcto, nos devolverá el siguiente mensaje:

Finalmente, creamos el Server dando click en Build.



Guardamos…

Hemos terminado!

Ahora solo queda encriptar nuestro server y pasarlo a algún remoto, o en donde lo deseen ejecutar.

Les enseñare una captura de cómo se ve un panel que ya ha capturado passwords:

Program	Url / Host	Login	Password	Computer	Date
CuteFtp	[redacted]	[redacted]	[redacted]	[redacted]	2010-10-09 11:04:07
CuteFtp	[redacted]	[redacted]	[redacted]	[redacted]	2010-10-09 11:04:07
CuteFtp	[redacted]	[redacted]	[redacted]	[redacted]	2010-10-09 11:04:07
CuteFtp	[redacted]	[redacted]	[redacted]	[redacted]	2010-10-09 11:04:06
Firefox	[redacted]	[redacted]	[redacted]	[redacted]	2010-10-09 11:04:06
Firefox	[redacted]	[redacted]	[redacted]	[redacted]	2010-10-09 11:04:06
MSN Messenger		[redacted]	[redacted]	[redacted]	2010-10-09 11:04:05
MSN Messenger		[redacted]	[redacted]	[redacted]	2010-10-09 11:04:05
MSN Messenger		[redacted]	[redacted]	[redacted]	2010-10-09 11:04:05
Firefox	[redacted]		[redacted]	[redacted]	2010-10-08 17:56:21
MSN Messenger		[redacted]	[redacted]	[redacted]	2010-10-08 17:56:21
MSN Messenger		[redacted]	[redacted]	[redacted]	2010-10-08 17:56:21
MSN Messenger		[redacted]	[redacted]	[redacted]	2010-10-08 13:45:45

Espero que en esta entrega hayan aprendido lo que es un Stealer y su funcionamiento.

Este material no es expuesto para que todos roben pass, sino para que lo tengan en cuenta por si ven alguno de estos Stealers sueltos por ahí, y ser precavido para no ejecutarlo y caer en ellos.

Bueno, Como siempre agradezco a todos los lectores. También les agradezco enormemente a los que visitan mi blog, ya que me motivan a seguir escribiendo para ustedes.

Agradecimientos especiales:

Fakedo0r (Gran amigo mio)
P0is0n-123 (Administrador de indetectables.net)
El-Cirujano (Usuario y colaborador de indetectables.net)
Cygog (Gran colega mio)

Nos vemos en la próxima entrega que espero que sea pronto!

ANTRAX

www.antrax-labs.net