OPTIX & BIONET

Hemos recibido algunos e-mails de amigos lectores que quieren integrarse en el mundo de los troyanos, pero nos comentan que no saben por dónde empezar. Ven muchos datos en esta web, pero les falta la mínima base de conocimiento en la materia de los troyanos para seguir las explicaciones. Bien, pues en este tutorial deseo empezar desde cero. ¿Qué es lo primero que hay que hacer?. ¿Y después?. Todo está aquí. Sólo para principiantes.

Usted quiere espiar un ordenador y desea usar para ello un troyano. ¿Por dónde debe empezar?.

Bien, lo primero que vamos a hacer es elegir nuestro programa de espionaje. Para ello vamos a pensar primero en qué datos o qué acciones queremos llevar a cabo con el ordenador espiado. Si sólo queremos recoger todo lo tecleado por la víctima y no lo queremos hacer en tiempo real, podemos optar por un keylogger offline.

Un keylogger offline es muy seguro porque no expone nunca nuestra IP, ya que nuestro ordenador en verdad nunca se conecta al ordenador espiado. Simplemente lo que hace el keylogger es volcar cada cierto tiempo que le especifiquemos, todos los datos logueados a una cuenta de e-mail que podremos visitar cuando queramos. Veasé el artículo sobre keyloggers si quiere saber más sobre ellos.

Si además de recoger todo lo tecleado, queremos intervenir activamente en el ordenador espiado, entonces tendremos que optar por un troyano. Hay excelentes troyanos en Internet por los que no tendremos que pagar nada. También hay troyanos de pago (shareware) que no suelen ser detectados por los antivirus. Estos troyanos suelen advertir de su instalación, y por tanto no son apropiados para espiar un ordenador al que Usted no puede acceder físicamente. Si tiene que espiar el ordenador de una oficina a la que Usted accede regularmente, entonces es muy bueno un troyano legal o shareware, porque los antivirus nunca lo detectarán.

Si Usted lo que desea es espiar un ordenador físicamente alejado, entonces hay que optar por los troyanos convencionales. En este caso hemos de preocuparnos antes de hacerlo indetectable a la mayoría de los antivirus. Aunque lo primero es editarlo con nuestras preferencias.

Ya sabemos que un troyano posee tres partes fundamentales:

*** Editor: Suele ser un archivo de nombre EditSever.exe.**

*** Cliente: Suele ser un archivo de nombre Client.exe o lleva el mismo nombre del troyano (por ejemplo, NetBus.exe).**

*** Servidor: Suele ser un archivo de nombre Server.exe. ¡Es el que infecta!.**

La parte que infecta es la del **servidor**. Esto quiere decir que la víctima habrá de hacer doble clic sobre ese archivo (en la mayoría de los troyanos es un archivo llamado **Server.exe**) para infectarse.

El **editor** abre un programa que edita o configura el **servidor**. En el **editor** habremos de introducir manualmente nuestro número de **ICQ** o nuestra cuenta de correo electrónico, amén de un servidor **SMTP** que sea válido. Recuerden que Ustedes deben seleccionar previamente el **servidor** en el **editor** para que los cambios tengan lugar (vea el artículo sobre **sub7**).

La notificación es muy interesante porque con ella podremos saber la IP de la víctima y cuándo está conectada a Internet (online). Habría que probar antes su eficacia desde el **editor**. Hay troyanos como **Optix Pro** que permiten realizar pruebas. Por ejemplo, fíjense en cómo deberemos hacer una prueba para comprobar si la notificación por e-mail funciona:

Ésta es la pantalla que Usted verá cuando abre el **editor** de Optix Pro (el archivo **Editor.exe**). En **Server File Path** Usted habrá seleccionado el servidor de Optix Pro (pulsando sobre el botón [**...**] y buscando el archivo **Server.exe**). Busque el botón **Notification** ahora (en la parte izquierda de la imagen) y púlselo. Luego pulse **Mail Notification** y fíjese en Mail Notification Settings. En **Mail Notification Enabled?** seleccione la casilla **Yes**. Ahora puede optar por elegir un servidor SMTP personalizado (yo no lo recomiendo), o puede hacer que el propio ordenador de la víctima posea su propio servidor **SMTP** local. Para este último caso, pulse **Local Relay Server Notification (No SMTP required)**. Ahora tendremos que introducir una dirección falsa de correo electrónico en el campo **Mail From**. Si se da cuenta, yo he introducido una inventada: **mi_cuenta_falsa@test.com**. ¿Para qué sirve esto?. Pues para que en su cuenta de e-mail Usted reciba la notificación de alguna dirección. En cambio, en el campo **Mail To** Usted debe poner su cuenta de correo electrónico verdadera donde desee recibir la notificación. Ahora viene lo importante. Antes de grabar todos estos datos en el **servidor** (en **Server.exe**) debemos probar si el método funciona. Para ello vamos a pulsar el botón **Send test email using selected options!**. Ahora Optix Pro va a tratar de enviar un e-mail de prueba a la cuenta de correo electrónico que Usted le ha especificado. Si Usted lo ha recibido, entonces puede estar seguro de que el método también va a funcionar en el ordenador de la víctima. Fíjese en el tipo de mensaje recibido, porque cuando reciba las notificaciones reales del troyano, van a ser casi idénticas.

**Nota: Cuando intentamos hacer una prueba con la opción Local Relay Server Notification (No SMTP required), es posible que nos salga un error. De la manera que nunca falla la prueba es introduciendo un servidor SMTP y su puerto (ver tutorial de Sub7 para saber dónde hemos de buscar los servidores SMTP). En otros troyanos como Net-Devil también se puede probar la notificación por ICQ. Este tipo de comunicación es más sencilla, aunque igualmente inestable. Si van a usar la notificación por e-mail, les recomiendo que se abran una cuenta en HotMail y utilicen el Messenger para saber los correos entrantes al instante.*

En las notificaciones veremos la IP de la víctima y el puerto que su ordenador tiene abierto. También mostrará otros datos como el nombre de la víctima o algunas cosas adicionales, dependiendo del troyano usado.

No se olviden siempre de guardar los datos introducidos en el editor. Para ello (en el caso de **Optix Pro**) pulse **Save Settings**. En otros troyanos será muy parecido (les recomiendo una vez más que lean nuestro tutorial de **Sub7**).

Ya tienen editado el **servidor** del troyano. Pero el problema es que muchos antivirus van a detectar el archivo **Server.exe** que Usted debe enviar a la víctima. Si un antivirus detecta el troyano, Usted puede tener problemas con la persona que lo ha recibido. ¿Verdad que a Usted no le sentaría nada bien recibir un troyano de un conocido?. Pues el siguiente paso es, por tanto, ocultarlo a los antivirus.

Ya es indetectable a la mayoría de los antivirus nuestro troyano. ¿Ahora qué hacemos?. Pues vamos a

enviárselo a la víctima. Aquí no hay tácticas infalibles. Cada uno hace lo que puede. Si Usted puede acceder físicamente al ordenador que quiere infectar, puede llevarse el **servidor** del troyano (**Server.exe**) en un disquete e introducirlo en la disquetera del ordenador espiado para seleccionar **Server.exe** y hacer doble clic sobre él. Si Usted no puede hacer esto, entonces debería enviarlo por e-mail a la cuenta de la víctima, haciéndole pensar a la víctima que se trata de cualquier aplicación que se le ocurra (así ya no "pica" casi nadie, pero todavía quedan ingenuos). También puede simular con un mensaje de error que el archivo está corrupto (esto se configura en el editor: vea para ello nuestro tutorial de **Sub7**). Este método también está muy en desuso. Puede buscar un error en las actualizaciones del **Internet Explorer** para aprovechar algún bug no parcheado (lea para ello nuestro tutorial de **Infectar por WEB**). O puede optar por "pegar" un archivo legítimo al **servidor** del troyano. De esta manera cuando peguemos un troyano a un juego, la víctima sólo verá en su pantalla la ejecución visible del juego, pero al mismo tiempo el troyano se habrá instalado silente en su ordenador. Para aprender a pegar troyanos a juegos u otros programas, lea nuestro artículo de **Binders**.

Los canales para la transmisión de troyanos son muy variados. Puede usar el correo electrónico (debe tener en cuenta que hay servidores de correo electrónico como **Hotmail** y **Yahoo** que poseen antivirus que alertan a los usuarios sobre los virus). También puede usar el **ICQ**, el **MSN**, los canales de **IRC**, etc. Sin embargo, el método más eficaz de todos es el **P2P**. Si Usted de veras quiere infectar a mucha gente (sin personalizar) entonces pruebe a introducir en su carpeta de archivos compartidos en el **KaZaA** un troyano pegado a un juego muy famoso, un famoso antivirus o un crack muy solicitado. Póngale un nombre muy llamativo, por ejemplo, **Crack_for_Panda.zip** o **Crack_FIFA2000.zip**. Espere pacientemente y verá cómo en pocos minutos empezarán a llegarle las primeras notificaciones de los primeros infectados. He de decirles que yo desapruebo completamente este tipo de acciones deplorables. Si Usted infecta a alguien para realizar una prueba, lo que inmediatamente debe hacer es eliminar el **servidor** del troyano del ordenador de la víctima. Siéntase satisfecho por simplemente probar que el método funciona y elimine todo rastro del troyano del ordenador de la víctima.

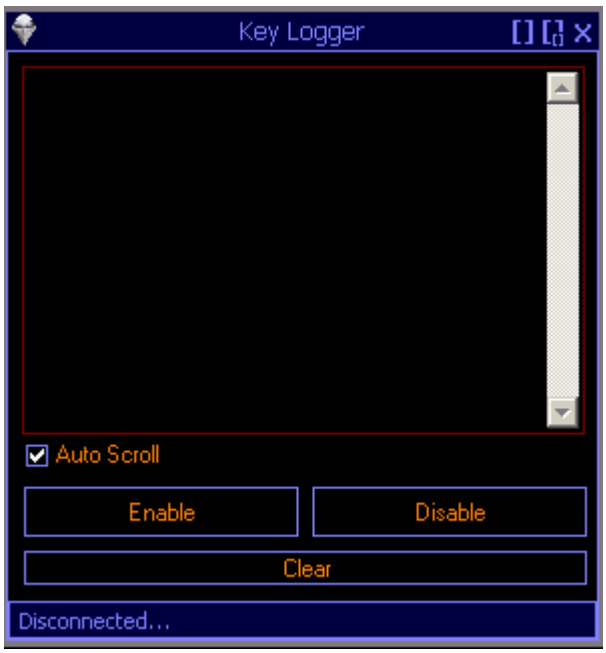
**Nota: Debemos entender la filosofía que subyace tras las redes P2P como KaZaA, WinMX, E-Donkey, etc, antes de proceder a infectarlas con troyanos. Estas redes son lo más democrático y solidario que existe en Internet. Mis archivos son de todo el mundo y los archivos de todo el mundo son míos. Nunca en la historia de la humanidad el sentimiento de compartir estuvo tan extendido como con estas redes. Si las atiborramos de troyanos, generaremos en los usuarios una actitud de desconfianza y egoísmo. Esta magnífica solidaridad se acabará porque nadie querrá ver sus ordenadores infectados. Seamos conscientes en todo momento de esto y respetemos las redes de P2P. La información aportada sólo es orientativa, nunca trato de animar a nadie a que lo haga. Mi consejo personal es que pasen de infectar este tipo de redes.*

Tenga en cuenta también que si Usted abusa de las notificaciones de los troyanos, su servidor de correo electrónico le puede bloquear la cuenta, su servidor de **ICQ** le puede deshabilitar los **ICQ Pagers,** y si instala el método **CGI** en su web, puede tener problemas con la Policía si alguien le denuncia. Con la entrada en vigor de la **LSSICE**, está prohibido mostrar direcciones IP ajenas en una web.

Cuando Usted reciba una notificación vía **e-mail** o vía **ICQ**, Usted deberá copiar la IP que ve en la notificación (un número del tipo **xxx.xxx.xxx.xxx**; donde **xxx** es cualquier cantidad desde **0** a **255**) al **cliente** del troyano (vea nuestro manual de **Sub7** para identificar el **cliente** y saber cómo se usa: en **Optix Pro** el **cliente** es **Client.exe**). Compruebe también si el puerto (**Port**) es el correcto y pulsemos en el botón **Connect**.

Una vez esté en el ordenador de la víctima, Usted no verá la pantalla de la víctima tal y como ella la ve (a menos que realice una captura de pantalla o **Screen Capture**). Lo que tendrá es una ubicación de los directorios de la víctima. Podrá abrir sus archivos, copiarlos a su ordenador, borrarlos, modificarlos, etc. Tendrá todas sus contraseñas y con el keylogger, podrá espiar todas sus conversaciones de chat, así como todos los documentos que escriba (aunque no los guarde o los codifique). Si Usted, por ejemplo, decide apretar el botón en su **cliente** para abrir el CD-ROM, Usted nunca verá esa acción en pantalla (se la tendrá que imaginar, aunque podemos estar seguros de que si el troyano funciona, el CD-ROM ha debido de abrirse).

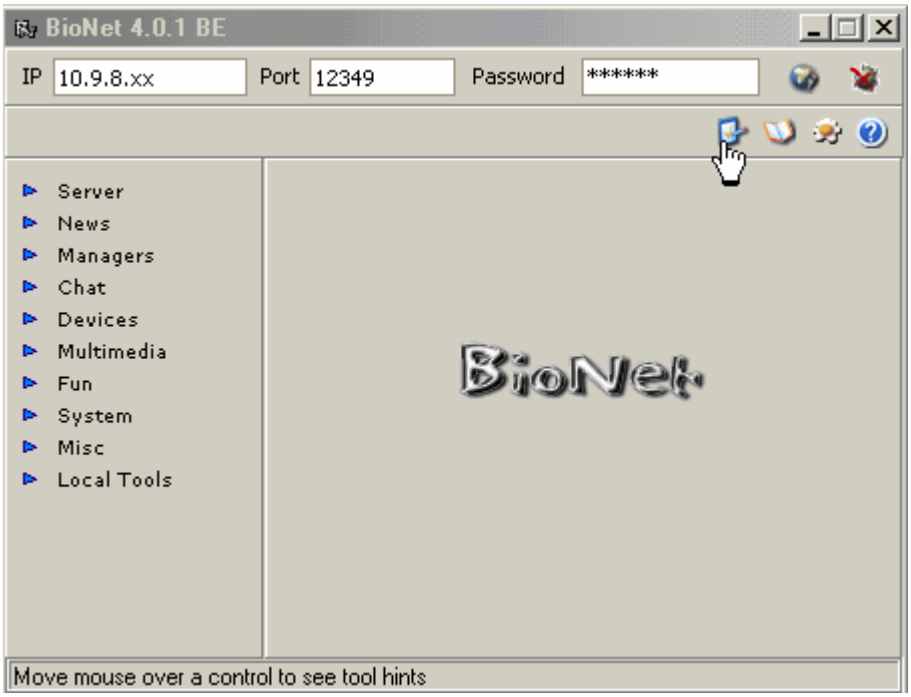
La pantalla con la que Usted va a jugar es la del **cliente**. Desde ese entorno gráfico lo va a manejar todo. Por ejemplo, si Usted activa el keylogger, esto es lo que verá en su pantalla en el **cliente** del troyano **Optix Pro**:



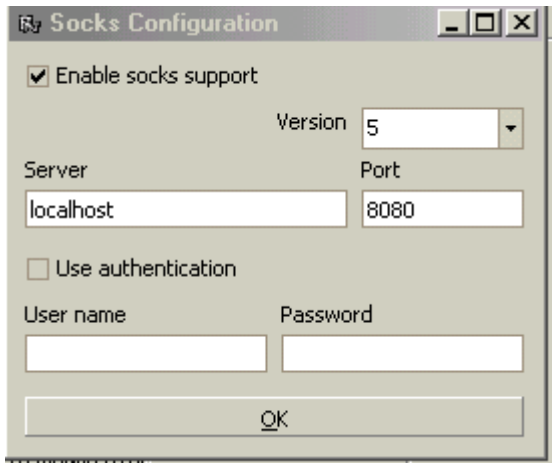
En ese espacio en negro que existe debajo de la palabra **Key Logger** va a ver Usted las palabras que está tecleando la víctima (tras pulsar el botón **Enable**). Es eso lo que ve.

Por supuesto, puede utilizar un proxy para ocultar su verdadera IP. De esa manera la víctima nunca se apercibirá de que es Usted quien está detrás del espionaje. Esto no es fácil hacerlo con cualquier troyano, pero hay algunos que lo permiten de una manera muy sencilla. Tal es el caso de **Bionet** en cualquiera de sus versiones.

Abra el cliente de **Bionet** y vea esta pantalla:



Observe donde he colocado el cursor (la mano que señala un pequeño icono). Pulse precisamente sobre ese pequeño icono. Ahora tendrá dos opciones más: pulse sobre **Proxy Setup**. Esto es lo que verá ahora:



Deberá marcar la opción **Enable socks support**. Si dispone del programa **Proxomitron**, también debe configurar los demás datos de la misma manera que aquí ve. Al final pulse sobre **OK** y ya estará entrando en el ordenador de la víctima a través de un proxy. Para configurar **Proxomitron** lea nuestro tutorial **Proxies**.

Como han podido comprobar en este tutorial no hay recetas milagrosas para el uso de un troyano. Cada uno de estos programas tiene sus características concretas y cada uno de nosotros también tiene su manera de usar los troyanos. Espero haber servido de ayuda a esos amigos lectores de la web que nos solicitaban ayuda para usar un troyano por primera vez. Y sobre todo recuerden que el uso de estos programas para el espionaje está tipificado en el Código Penal de muchos países como delitos. Sean prudentes en su utilización.

Autor: **Coolvibes**

Página: Indetectables.com.ar