Manual Básico para trabajar con un KeyLogger

Disclaimer

Queda bajo total responsabilidad del lector cualquier tipo de uso que se le de a esta información.

El autor de esta obra queda libre de todo tipo de responsabilidad por daños materiales o intangibles producto de la mala interpretación o uso del contenido, defectos en el software o técnicas derivadas utilizadas, incumplimiento de normas de seguridad y/o morales, etc. ya que este material es meramente informativo y el único objetivo del mismo es brindar una orientación básica hacia el tema del manejo de keyLoggers.

Intro

En vista de la inseguridad que actualmente tenemos que padecer en Argentina e internacionalmente gracias a las nuevas tecnologías, precio aparente que debemos pagar para "evolucionar", me sentí obligado a registrar la metodología de "espionaje" utilizada actualmente para realizar un seguimiento oculto en una PC, osea un manual básico para trabajar con KeyLoggers.

Sencillamente voy a explicar como trabajar con un KeyLogger en especial, sin embargo servirá de experiencia y panorama informativo y práctico, para trabajar con cualquier otro KeyLogger ya que los principios básicos de trabajo de este tipo de software son los mismos en la mayoría.

Este tipo de software funciona muy bien, el problema es el uso que se le da ya que nos brinda mucho poder a la hora de invadir la privacidad de los demás operadores de una PC.

Como dentro de esta introducción mencioné la palabra "seguridad" dentro de un contexto que actualmente preocupa, es directamente ése el uso que aconsejo dar a este manual, un uso para preservar la seguridad en nuestra familia, empresa o entorno en particular y una luz de alerta para cuando utilizamos información confidencial en PCs de acceso público ya que nosotros podemos ser víctimas de un "espionaje".

Personalmente creo que hay que respetar la privacidad y los espacios recreativos o laborales de las demás personas, en determinadas circunstancias o la mayoría de ellas hasta es ilegal violarla o también moralmente incorrecto. Pero si tenemos el presentimiento o pruebas contundentes de que nuestros niños o adolescentes están bajo cierta amenaza en particular y la seguridad de ellos esta en nuestras manos, podemos hacer algo.
Y que yo escoja utilizar éste método en particular, no significa bajo ninguna circunstancia que todos deban hacerlo y sea la solución para todo el mundo, ojo, este manual es solo un registro práctico de un método que a algunos les puede servir y a otros no.

Así que, espero que le den a este material un buen uso y les sirva. Yo se que a muchos que pasan o han pasado por problemas de pedofilia o inseguridad a través de chats o redes sociales, a través de Internet precisamente, este material les hubiese ayudado o les ayudará mucho.

Esta guía esta basada en software que trabaja bajo Windows XP, el sistema operativo más común.

KeyLogger

Para entender lo que es un KeyLogger debemos entender lo que es un Loggin o Loggeo ya que de ahí viene la palabra; Key en ingles significa llave, tecla, clave, botón, interruptor, etc… depende en el contexto en que se aplique será su significado, obviamente. En este caso Key se refiere a tecla (Keyboard; teclado) y Loggin, logging, logg, logger, log, loggeo, logueo, etc. se refiere a registro, registrar, registrador, etc.
Entonces KeyLogger significa "registra-teclas" , "registrador de tecleos" o "registrador de tipeos"…

El KeyLogger es un software, un programa de computación que registra cada cosa que sucede y se visualiza en el monitor de una PC o Notebook, exacto, no registra únicamente la manipulación del teclado o Mouse (cosa que hacían los primeros KeyLoggers), sino que puede registrar mediante capturas programadas todo lo que sucede frente a la cara del operador de la PC.

Además de registrar lo que se visualiza en el monitor, puede registrar qué sucede con el software del equipo, si se borran datos, si se ejecuta este o aquel programa, etc. y en que horario sucede cada cosa.

El KeyLogger registra en videos, texto e imágenes todo lo que sucede. Graba, captura de forma programada (saca fotos) y anota en archivos de texto absolutamente todo lo que se necesita para realizar un seguimiento al uso de un equipo de computación.

Estos programas, además pueden ocultarse y trabajar sin que el o los operadores de la PC se den cuenta. Principalmente ése es el objetivo de los KeyLoggers, espiar y recaudar información a escondidas.

Algunos también pueden enviar la información obtenida a la casilla de E-Mail que se le indique de forma automática y programada.

Si vamos a un Cybercafé o a la sala de PCs de alguna institución pública o de acceso público, o por ejemplo a la sala de computación de la facultad, biblioteca, etc. Es probable que halla un KeyLogger instalado y estemos siendo víctimas de un espionaje. Y no digo que seamos espiados por el responsable de la sala o de las PCs, sino que cualquier usuario ajeno a la propiedad de las PCs pudo haber dejado instalado un Keylogger para más tarde regresar y adquirir información personal de los que usaron las PCs… es probable pero no significa que suceda en todos lados, es bueno saberlo pero no hay que entrar en paranoia, hay que estar prevenidos.

Y no hay nada que podamos hacer, que yo conozca, que sea 100% efectivo para evitar ser espiados ya que existe una gran variedad de KeyLoggers y programas que pueden ocultarse y registrar hasta las coordenadas en que se desplazó el Mouse y cuanto tiempo se detuvo y en que pixel.
Existen técnicas de evasión o prevención pero ese es otro tema mas amplio; podes prevenirte hasta cierto punto pero es probable que te espíen en cualquier pc de acceso público además, como veremos, es muy fácil usar este tipo de software.

Como evadir un KeyLogger

Afortunadamente a alguien se le ocurrió algo para evadir hasta cierto punto a los KeyLoggers, algo que se llama Teclado Virtual.

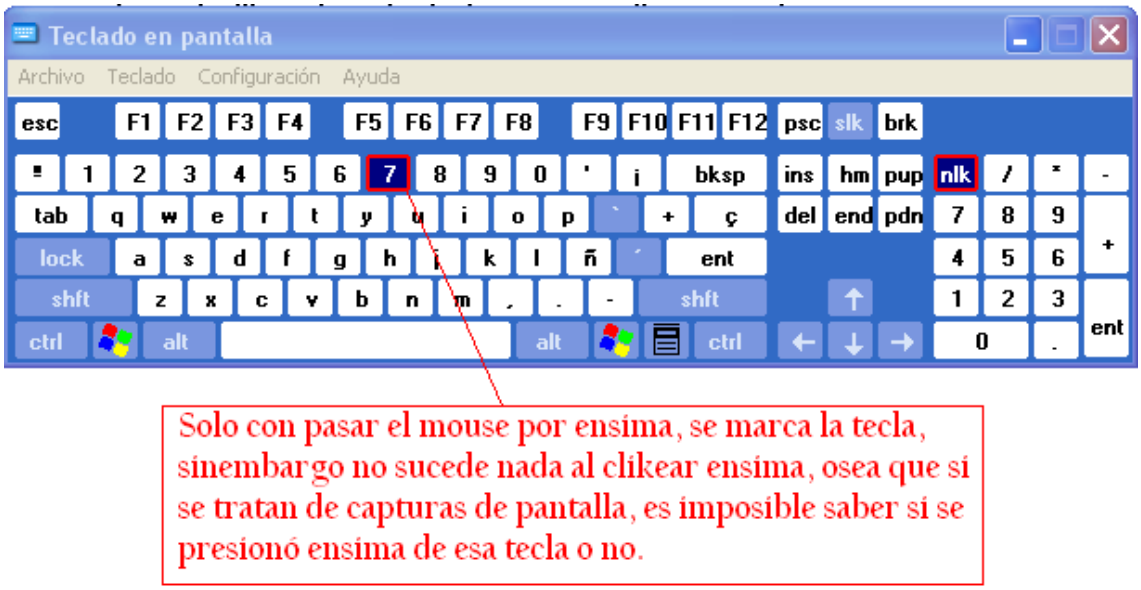
Ojo, solo sirve para evitar que queden registradas contraseñas o passwords de esas que al ingresarlas se visualizan asteriscos "******". Casi todos los programas o páginas que necesitan contraseña, la ocultan bajo asteriscos para que no se vean ocasionalmente por algún desconocido que pase cerca nuestro, pero los KeyLoggers pueden capturar la información de cuales fueron las teclas usadas para escribir la password.

El Teclado Virtual sirve para evadir a los KeyLoggers que registran las teclas que se presionan para ingresar una contraseña, password o palabra secreta.

Por ejemplo, accedemos al teclado virtual de Windows XP yendo a menú inicio/ ejecutar y luego escribiendo osk y presionando la tecla enter.

El teclado virtual es un programa que se encuentra en nuestra PC, teniendo en cuenta que utilizamos Windows XP, y sirve para escribir o teclear con un teclado gráfico utilizando el Mouse. Cuando se abre el programa aparece un teclado virtual y podemos ir clikeando en las teclas que necesitamos presionar.

Al utilizar el teclado virtual, evadimos el logueo gráfico de la PC, veamos porqué…



Tal cual; si pasamos el Mouse sobre el teclado virtual, se marcará la silueta de cada tecla sobre la cual nos desplacemos, y al clikear sobre ellas gráficamente no sucede nada, osea que al clikear sobre la tecla del teclado virtual no cambia de color ni parpadea ni hace nada que delate visualmente el clik con el botón del Mouse. Esto significa que el KeyLogger, aunque esté registrando en un video los movimientos del Mouse, jamás se enterará cual de todas esas letras sobre las cuales el Mouse se desplazó fue o no presionada.

Este sistema de teclado virtual que trae Windows, se puede encontrar también y de manera opcional en paginas webs de instituciones bancarias o de empresas en las cuales se maneja dinero o cierta información que debe ser totalmente confidencial.

Asíque, siempre que veamos que se nos ofrece un teclado virtual, o veamos el dibujo del mismo promocionando su servicio en algún sitio, estamos frente a una opción para preservar

nuestra seguridad, y si, todos los que conozco que funcionan online son gratuitos y forman parte de la seguridad del sitio.
Y ahora ya sabes, a pesar de que al Teclado Virtual no este disponible en todos los sitios online, podes utilizar el que trae Windows, por ejemplo para ingresar con password a tu casilla de E-Mail o cuenta de "red social", del banco o cualquier sistema que te lo exija.

Resumiendo la primer parte del manual

El KeyLogger es un programa de computación que registra todo lo que sucede cuando una PC está en funcionamiento. Graba la información en videos, imágenes y texto, con hora y fecha y no se limita a registrar lo que se observa en el monitor, sino que también puede grabar información de lo que sucede con el software.

Se le puede dar un mal uso en nuestra contra y podemos evadirlo hasta cierto punto con un teclado virtual, pero eso no es garantía de que estemos a salvo. Con el teclado virtual solo podremos ocultar nuestras contraseñas, pero lo que estamos viendo en la pantalla puede quedar grabado.

Cómo usar un KeyLogger

Voy a explicar como instalar, configurar y utilizar un KeyLogger conocido.

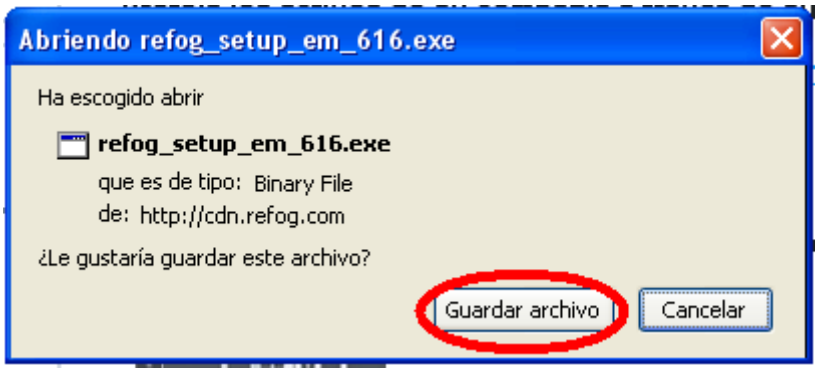
El KeyLogger que utilizaremos se llama Refog Employee Monitor y seguramente lo pueden encontrar 100% funcional en Internet ya que es muy conocido. También, y como veremos al final del manual, es recomendable el KGB Employee Monitor que también es de la familia de los Refog.

Si consiguen una versión 100% funcional, mejor.

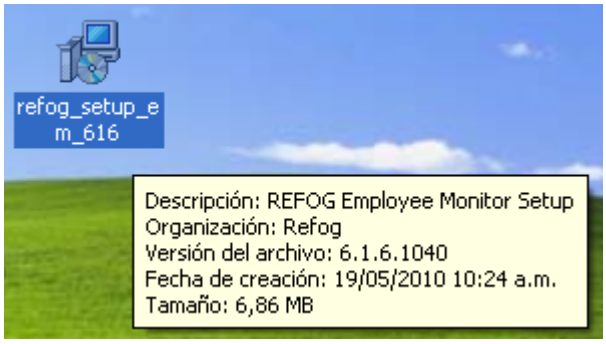
Para este manual vamos a utilizar la versión de prueba gratuita que encontramos en el sitio oficial del producto:

http://www.refog.es/employee-monitoring.html

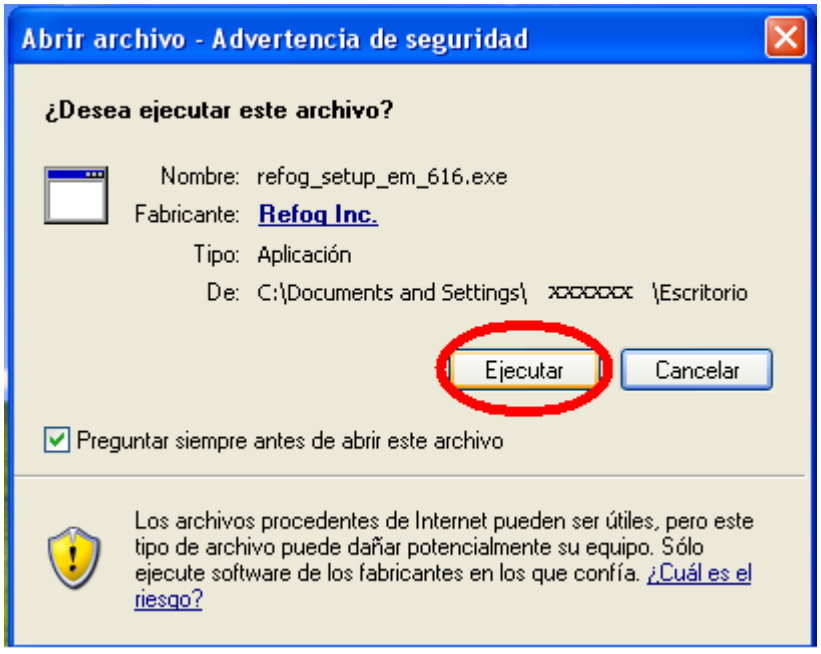
Ingresamos al link indicado y clikeamos en "Descargar prueba gratuita", luego guardamos el archivo.



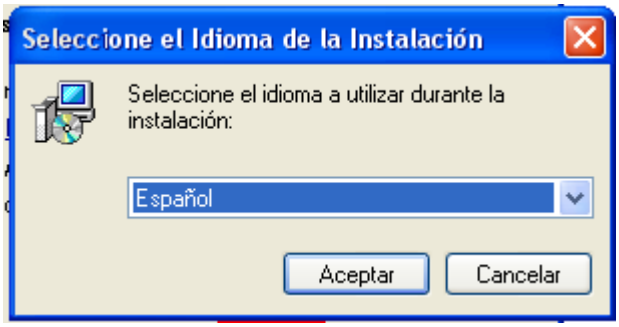
Ejecutamos el archivo descargado…



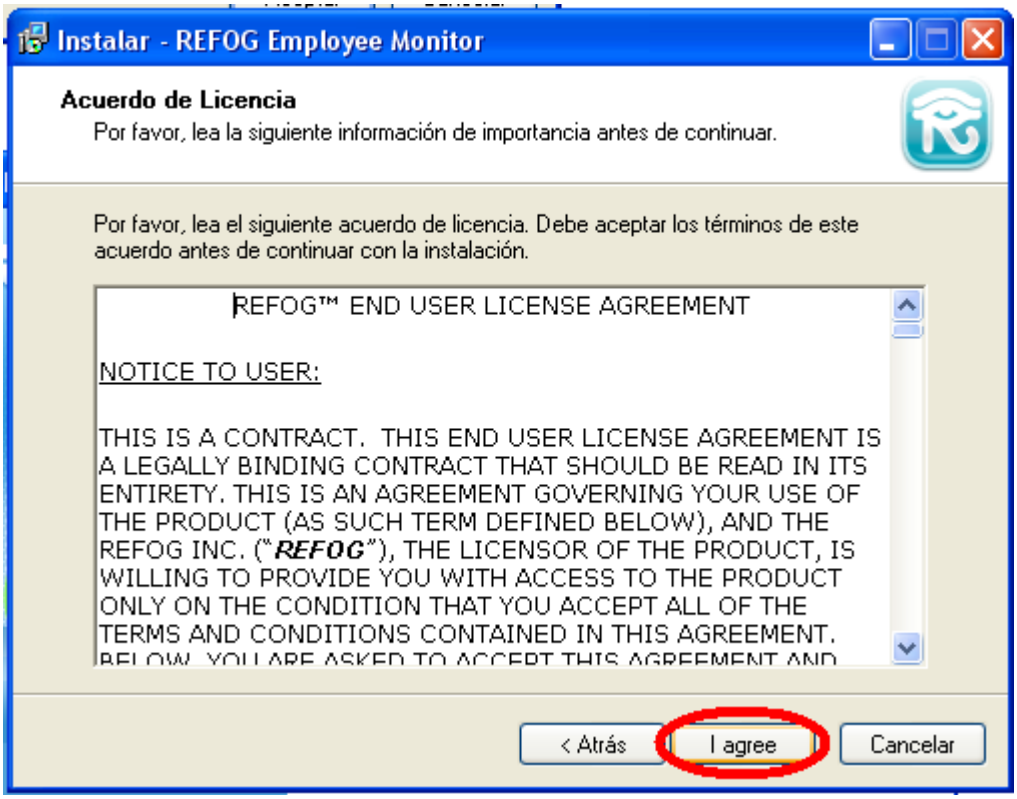
Y de este modo procedemos a su instalación…

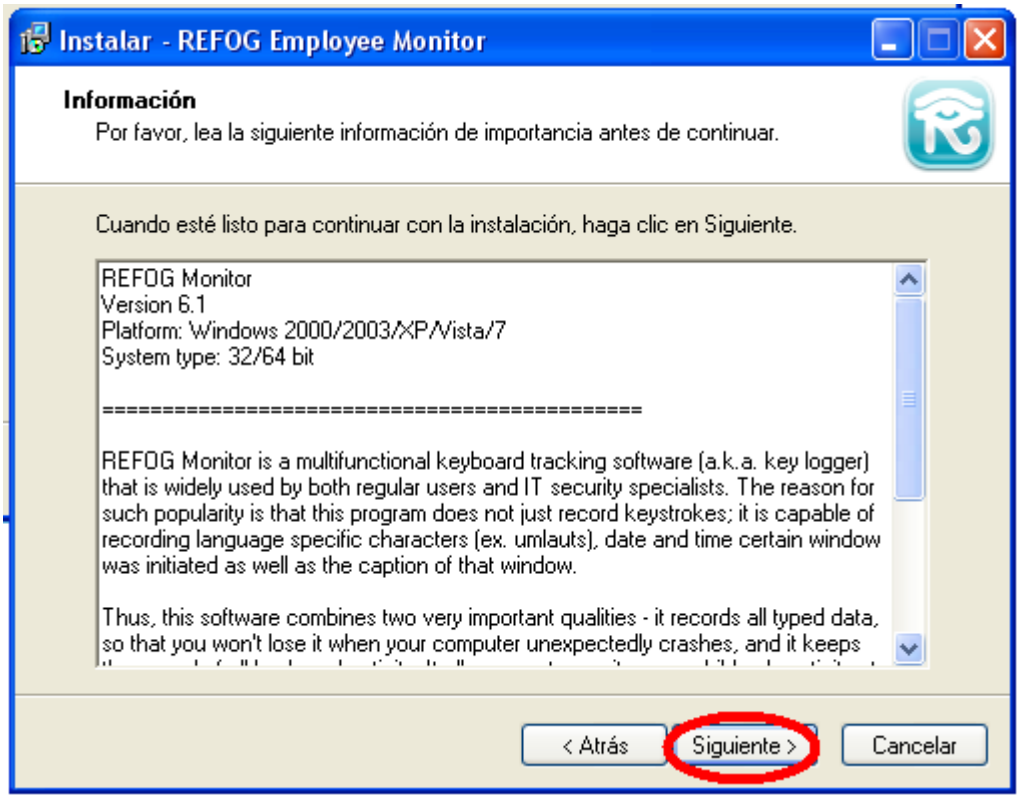


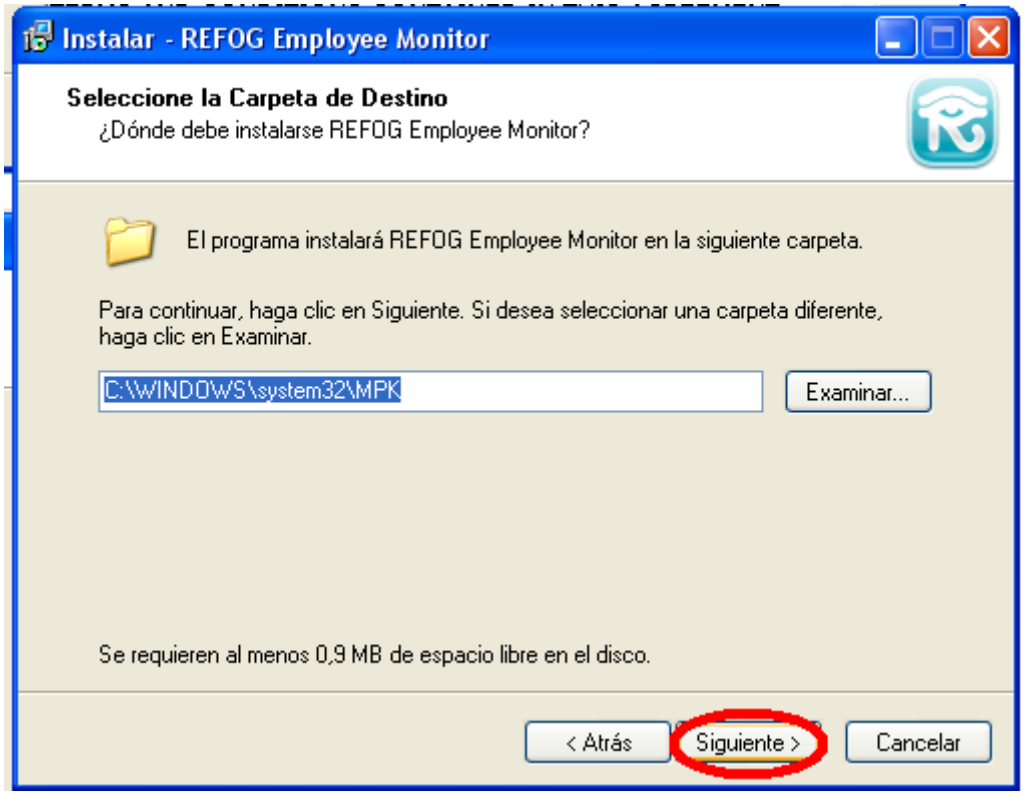
Seleccionamos el idioma…



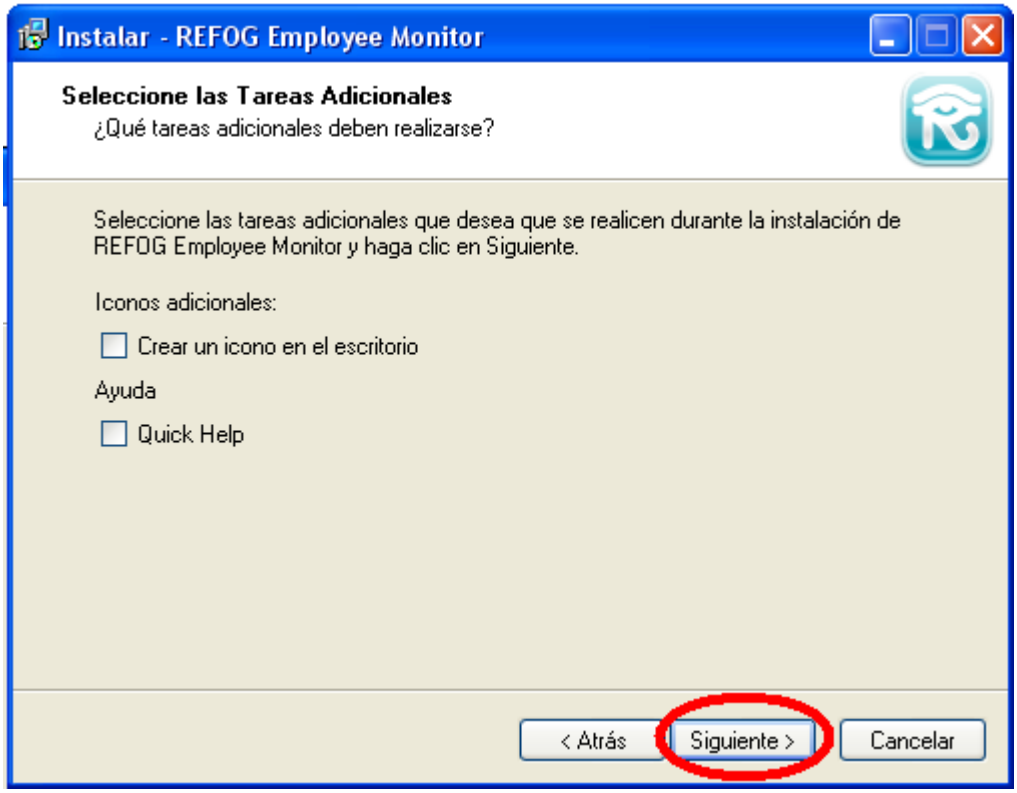
Y bien, se instala como un programa Standard… mas allá de eso siempre se recomienda leer todo, incluso los términos y condiciones o acuerdo de licencia antes de presionar en "Siguiente"…

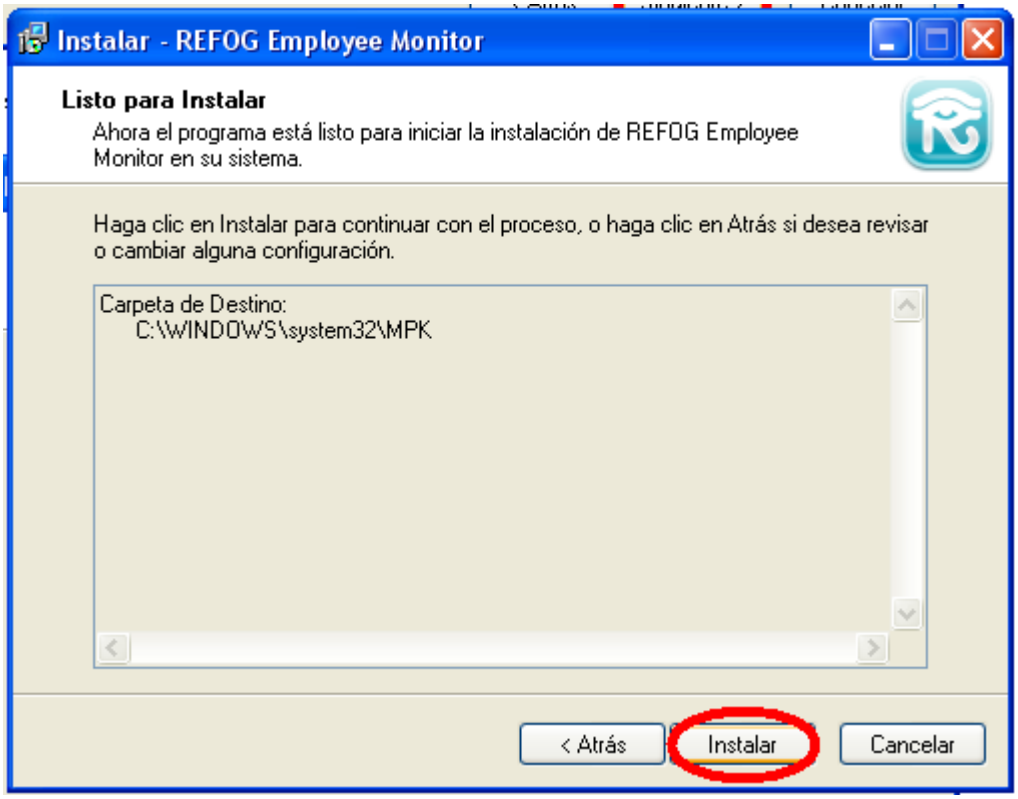

Instalar - REFOG Employee Monitor
Acuerdo de Licencia
Por favor, lea la siguiente información de importancia antes de continuar.
Por favor, lea el siguiente acuerdo de licencia. Debe aceptar los términos de este acuerdo antes de continuar con la instalación.
REFOG™ END USER LICENSE AGREEMENT
NOTICE TO USER:
THIS IS A CONTRACT. THIS END USER LICENSE AGREEMENT IS A LEGALLY BINDING CONTRACT THAT SHOULD BE READ IN ITS ENTIRETY. THIS IS AN AGREEMENT GOVERNING YOUR USE OF THE PRODUCT (AS SUCH TERM DEFINED BELOW), AND THE REFOG INC. ("REFOG"), THE LICENSOR OF THE PRODUCT, IS WILLING TO PROVIDE YOU WITH ACCESS TO THE PRODUCT ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT.
< Atrás
I agree
Cancelar


Instalar - REFOG Employee Monitor
Información
Por favor, lea la siguiente información de importancia antes de continuar.
Cuando esté listo para continuar con la instalación, haga clic en Siguiente.
REFOG Monitor
Version 6.1
Platform: Windows 2000/2003/XP/Vista/7
System type: 32/64 bit
==========
REFOG Monitor is a multifunctional keyboard tracking software (a.k.a. key logger) that is widely used by both regular users and IT security specialists. The reason for such popularity is that this program does not just record keystrokes; it is capable of recording language specific characters (ex. umlauts), date and time certain window was initiated as well as the caption of that window.
Thus, this software combines two very important qualities - it records all typed data, so that you won't lose it when your computer unexpectedly crashes, and it keeps
< Atrás
Siguiente >
Cancelar



Aconsejo no crear un icono en el escritorio para poder actuar totalmente encubierto…



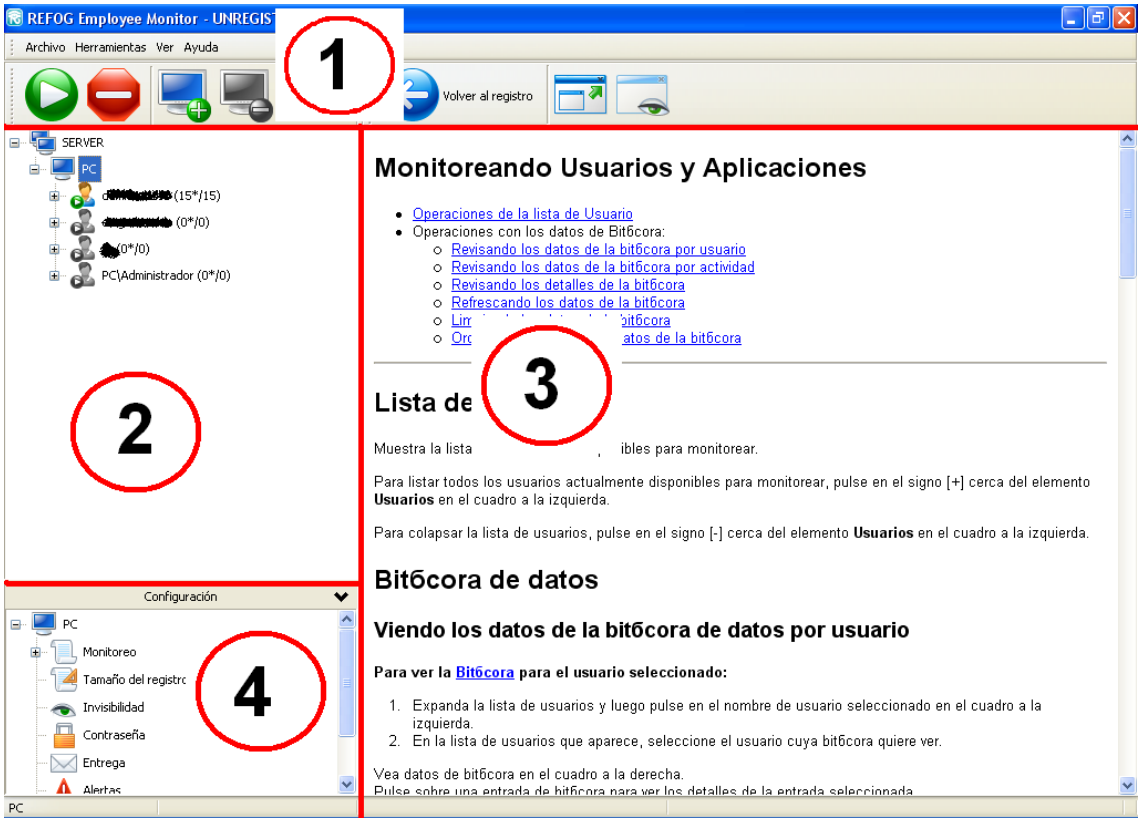


Luego de ver que se realiza automáticamente la instalación concluimos…

Ahora se abre el programa y, si usamos la versión que descargamos vamos a poder probarlo durante 30 días.

Clikeamos en "Ok" para probarlo…

Y veremos lo siguiente…



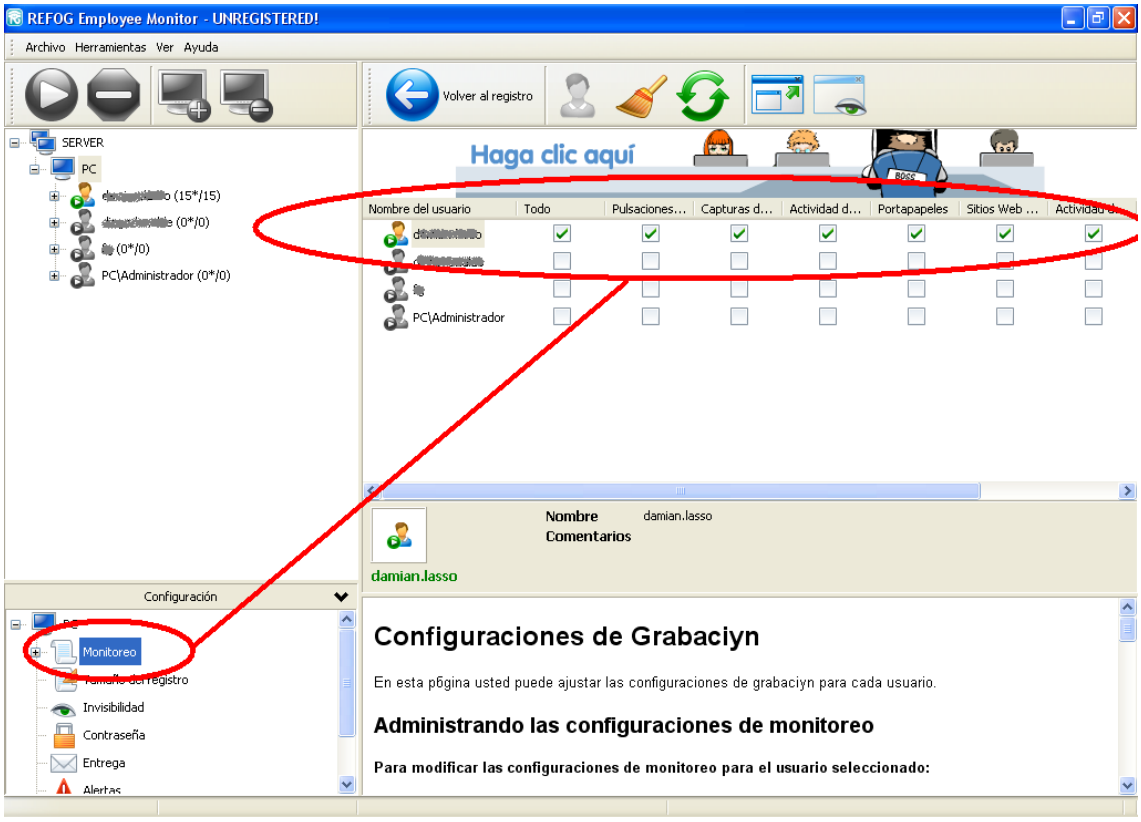
Donde;

1- Menú principal e Iconos de acceso rápido.

2- Organigrama en "árbol" de los posibles usuarios del equipo.
3- Panel de datos y registro (es donde veremos la información recaudada).
4- Organigrama en "árbol" de las características configurables del programa.

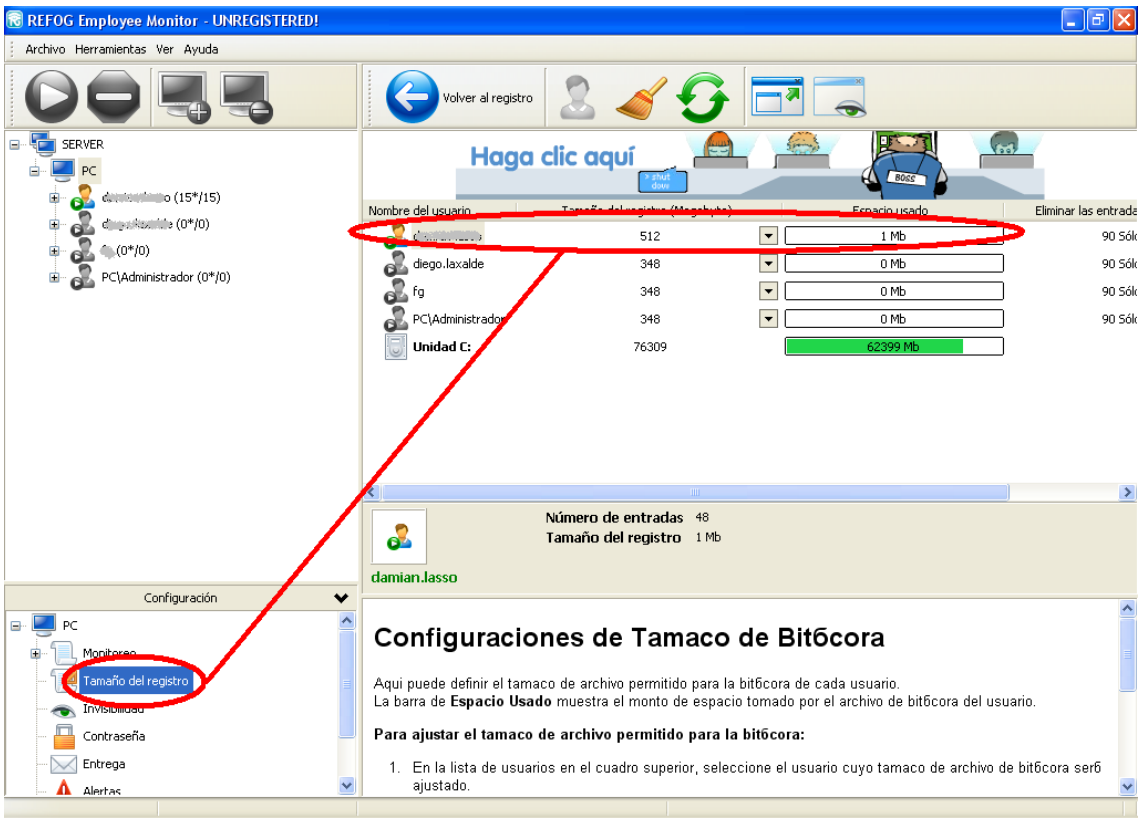
Como vemos, en el cuadrante Nº 2 tenemos a los posibles usuarios del equipo, osea a los que están reconocidos por Windows. Para iniciar el espionaje a cualquiera de ellos, simplemente pararse sobre el que sea o cada uno de ellos y clikear en el icono de acceso rápido con forma de botón de play. En este ejemplo solo hay habilitado el espionaje para un solo usuario, como vemos, el primero. Y si queremos deshabilitarlo, lo hacemos clikeando en el botón rojo.

Vamos a configurar el KeyLogger yendo en primera instancia al organigrama o panel de configuración que se encuentra en el cuadrante Nº 4, clic en el ítem "Monitoreo".

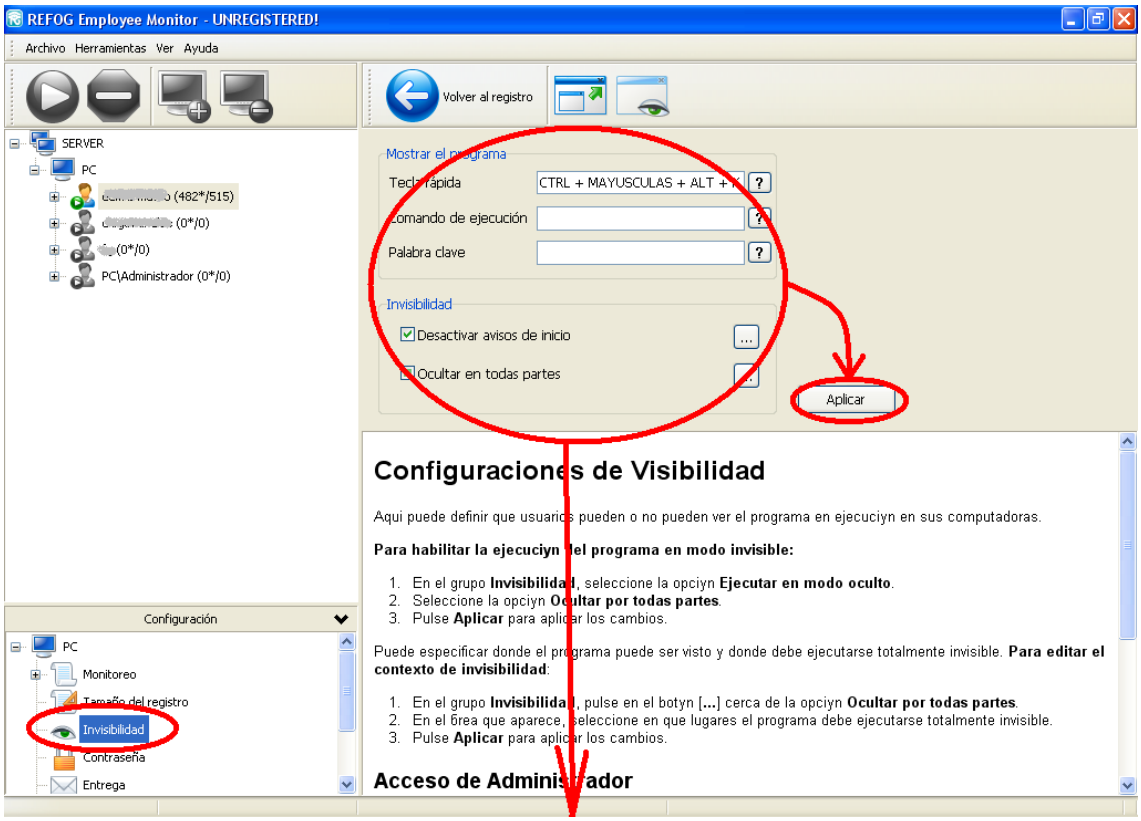


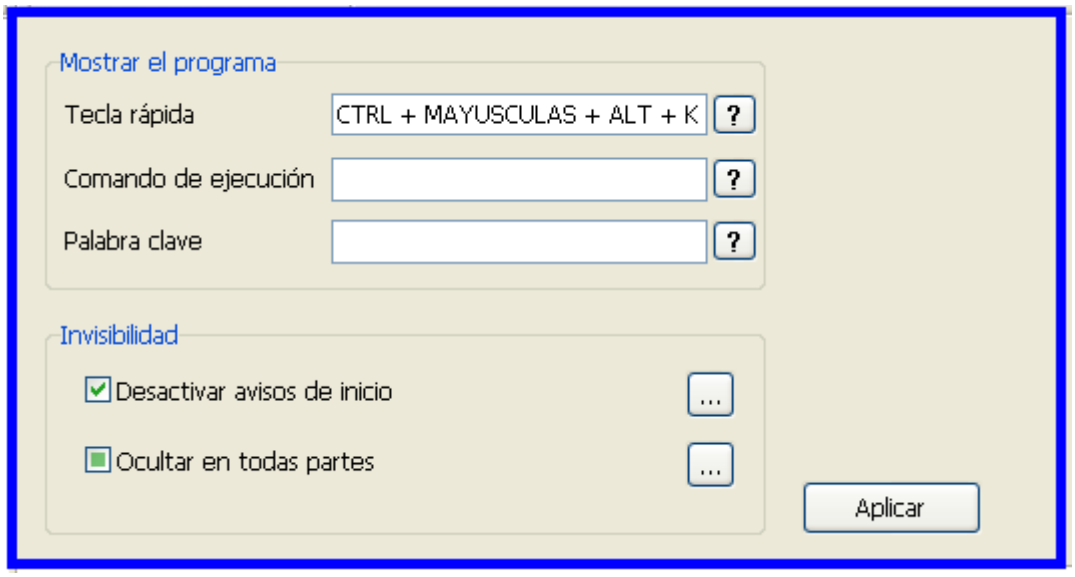
Al clikear en el ítem "Monitoreo", se nos abre un panel de configuración en el cuadrante Nº 3 y podemos tildar en las opciones que queramos, en este caso deseo monitorear todo por lo que tildo todo.

Luego, en el cuadrante Nº 4 seguimos con el siguiente ítem; "Tamaño del registro". Es muy sencillo, le indicamos al KeyLogger que capacidad de memoria tiene que reservar para el registro de tal o cual usuario. Cuanto más espacio mejor, mas cosas o mas rango temporal podrá almacenar…



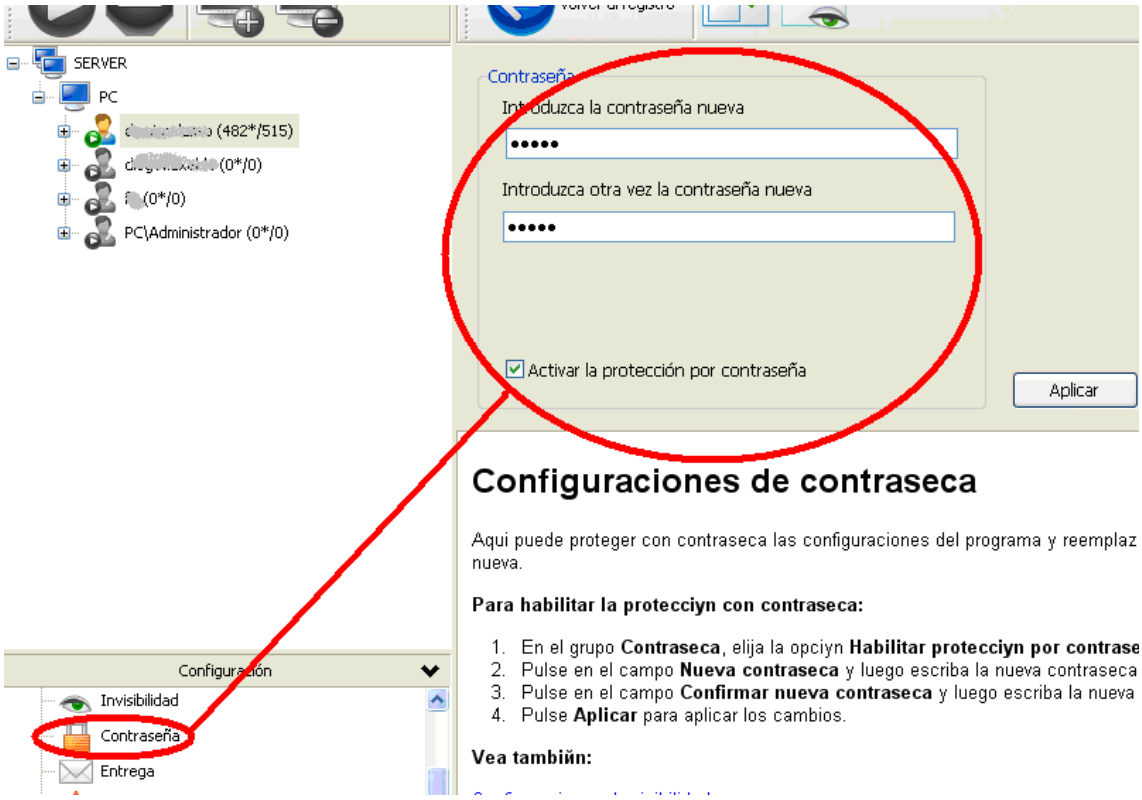
Ahora vamos a pasar al Ítem "Invisibilidad" en donde encontramos la configuración de la clave secreta para ingresar al KeyLogger, claro, para que solo nosotros tengamos acceso al registro. La clave secreta se usa cuando queremos revisar el registro que lleva el KeyLogger, si por ejemplo, luego de que finalice la semana o el día queremos ver qué cosas quedaron registradas, tecleamos la combinación de teclas secreta y se abrirá el KeyLogger con el registro.





Para que sea lo más invisible posible debemos dejarlo configurado de ese modo, y en "Tecla rápida" se puede inventar la combinación de teclas que quieras, no olvides que con esa combinación vas a poder acceder al KeyLogger para revisar los registros.
"Comando de ejecución" y "Palabra clave" nunca las utilicé asíque no se que tan efectivo será su uso.
Luego de la configuración de cada Ítem es fundamental no olvidarse de presionar el botón "Aplicar" ya que si no lo hacemos los cambios obviamente, no serán guardados.
Continuemos con la configuración…

Ahora vamos a el Ítem "Contraseña", en donde configuraremos una contraseña para el futuro acceso a la configuración del KeyLogger. Personalmente no uso esa opción.

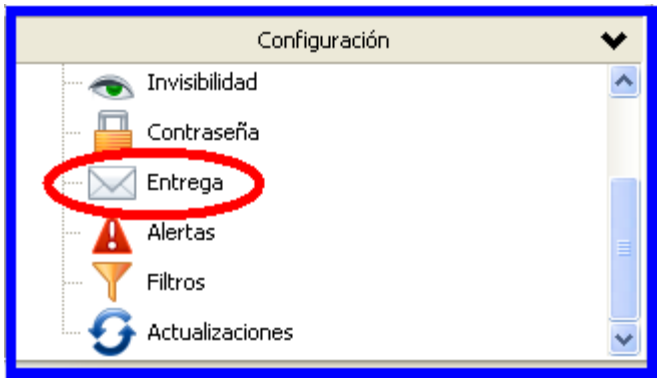


Luego de presionar el botón "Aplicar", continuamos configurando el Ítem "Entrega"…

En "Entrega" podemos configurar el envío de la información recopilada a nuestra servidor o casilla de email. Personalmente no uso esto ya que las PCs en donde deseo realizar el espionaje, están siempre a mano, sin embargo es bueno saberlo…

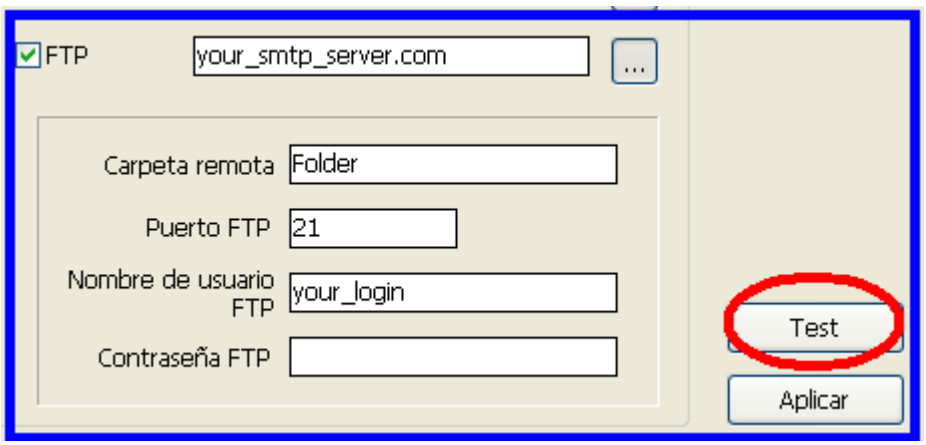
Podes configurar al KeyLogger para que te envíe la info. recaudada a tu casilla de E-Mail de forma automática!! esta buenísimo…

Entonces, vamos a…



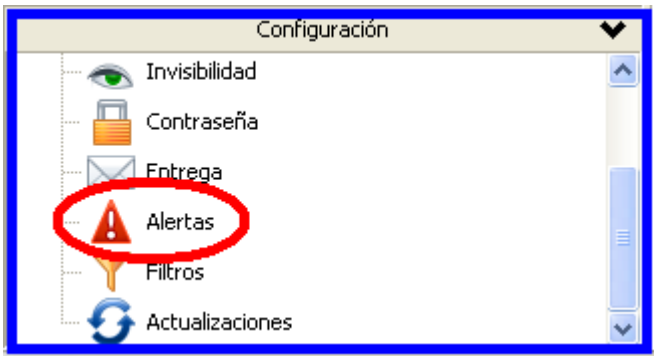
Ahora tenemos…

No es complicado, tenemos que configurar qué queremos que se nos envíe y a donde.
Si tildamos E-Mail se nos abrirá un panel para completar con los datos de nuestro correo y si tildamos FTP los datos de nuestro servidor…

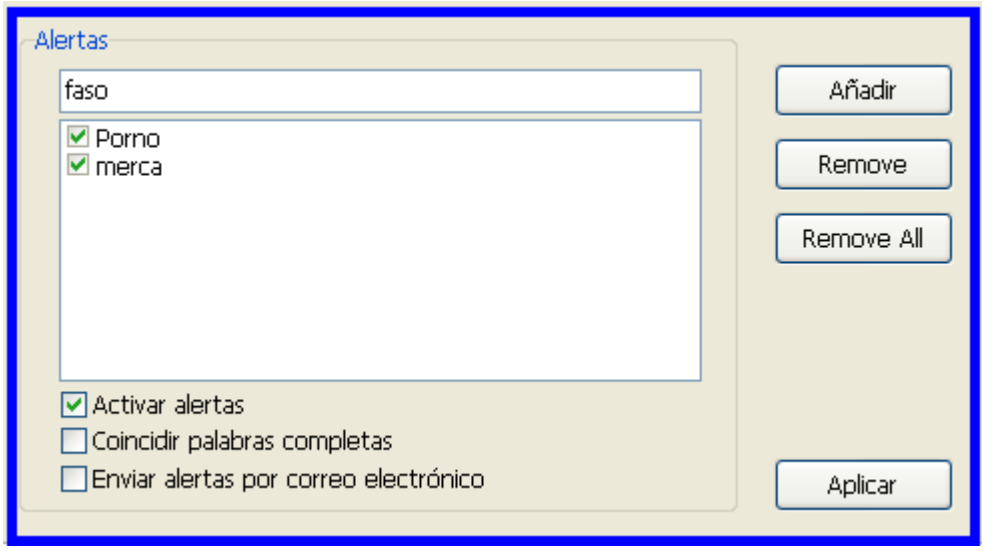


Y encima contamos con ese botón de testeo para verificar que el envío funciona Ok.

Seguimos en el cuadrante de configuración, y ahora vamos a "Alertas".

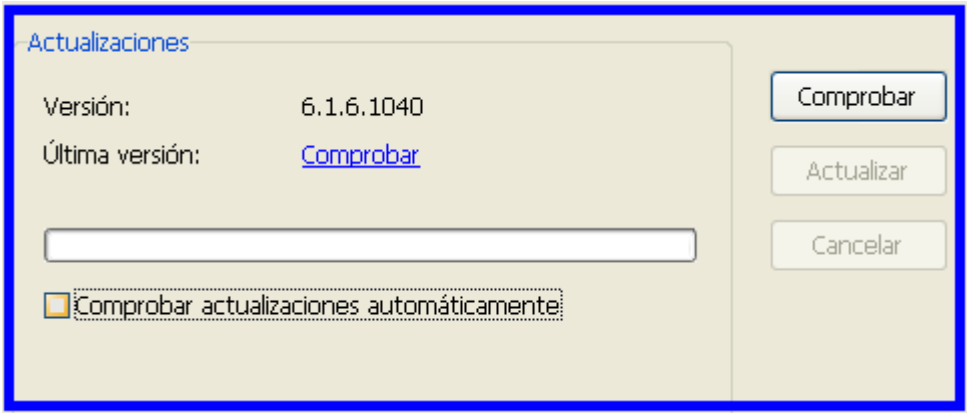


Y ahora, si queremos, podemos añadir palabras clave que activarán el registro del KeyLogger, en base a las palabras que grabemos se disparará una alerta interna y oculta, obviamente, para que el KeyLogger trabaje minuciosamente…



En base a nuestras dudas, temores o sospechas indicaremos las palabras adecuadas.

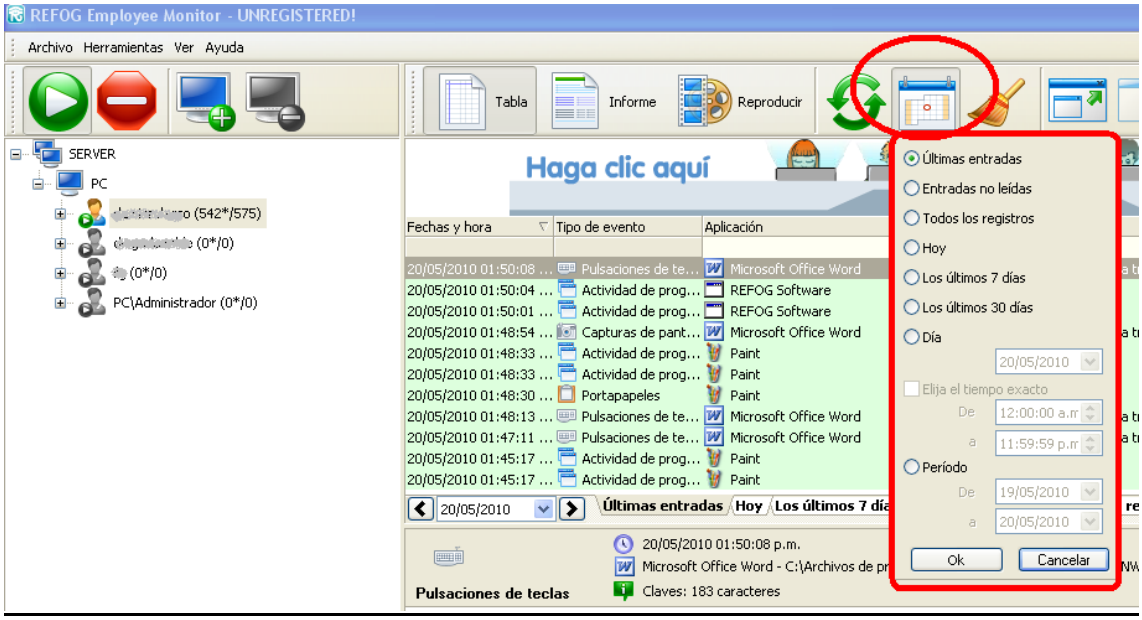
Los últimos 2 Ítems son "Filtros" y "Actualizaciones", no interesan mucho ya que no queremos filtrar nada ni actualizar nada, creo yo que ya que funciona correctamente no0 es necesario actualizarlo, eso si, hay que destildar "Comprobar actualizaciones automáticamente" para que no deba hacer ese trabajo extra.



Ok, ya está configurado el Keylogger, ahora veamos como hacer para acceder al mismo.

Acceso al registro del KeyLogger

Es muy fácil de utilizar, en el momento en que queramos echar un vistazo al registro, simplemente debemos presionar la combinación de teclas preconfigurada en el Ítem "Invisibilidad" y listo, Por ejemplo



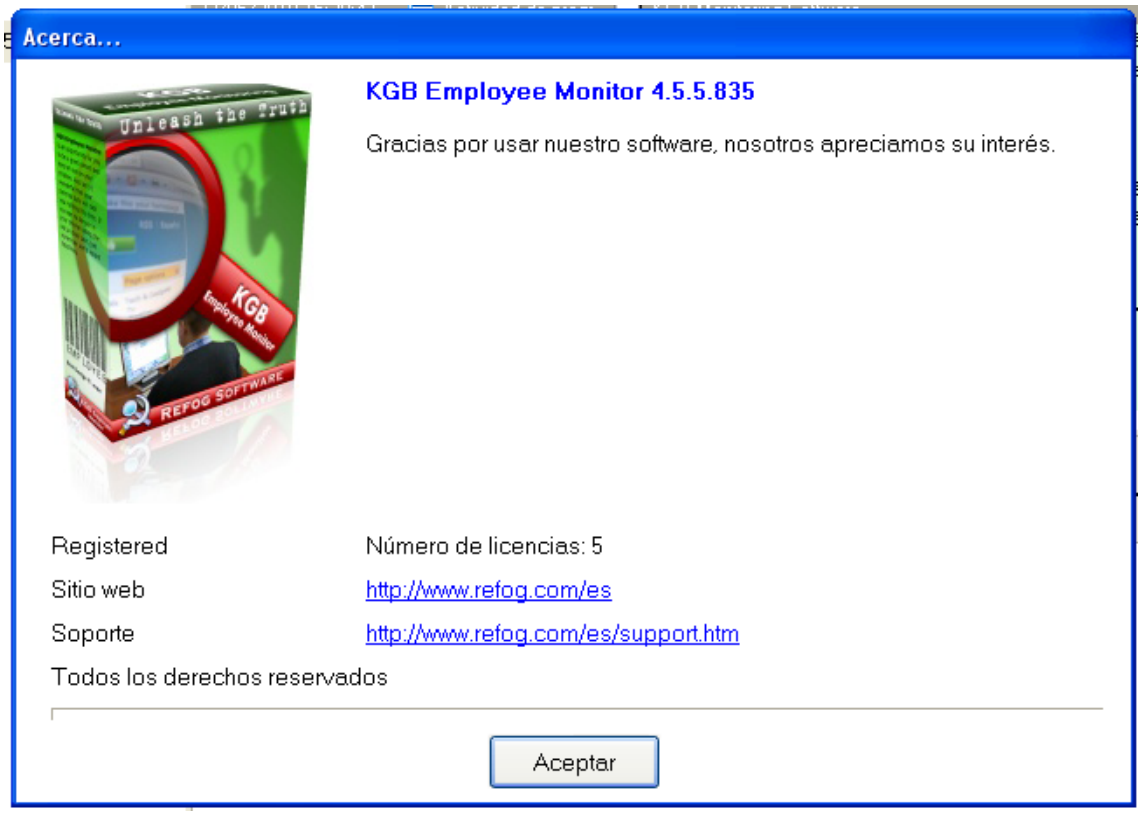
Para desinstalar el programa hay que ir al menú principal / Herramientas y luego Desinstalar. El desinstalador pedirá reiniciar el equipo y listo, no pasó nada…

Ahora bien, ya vimos como instalar, configurar y utilizar el Refog Employee Monitor, un KeyLogger muy poderoso y facil de utilizar de la familia de software de Refog.

Todos los KeyLoggers trabajan parecido, registrando y ocultándose.

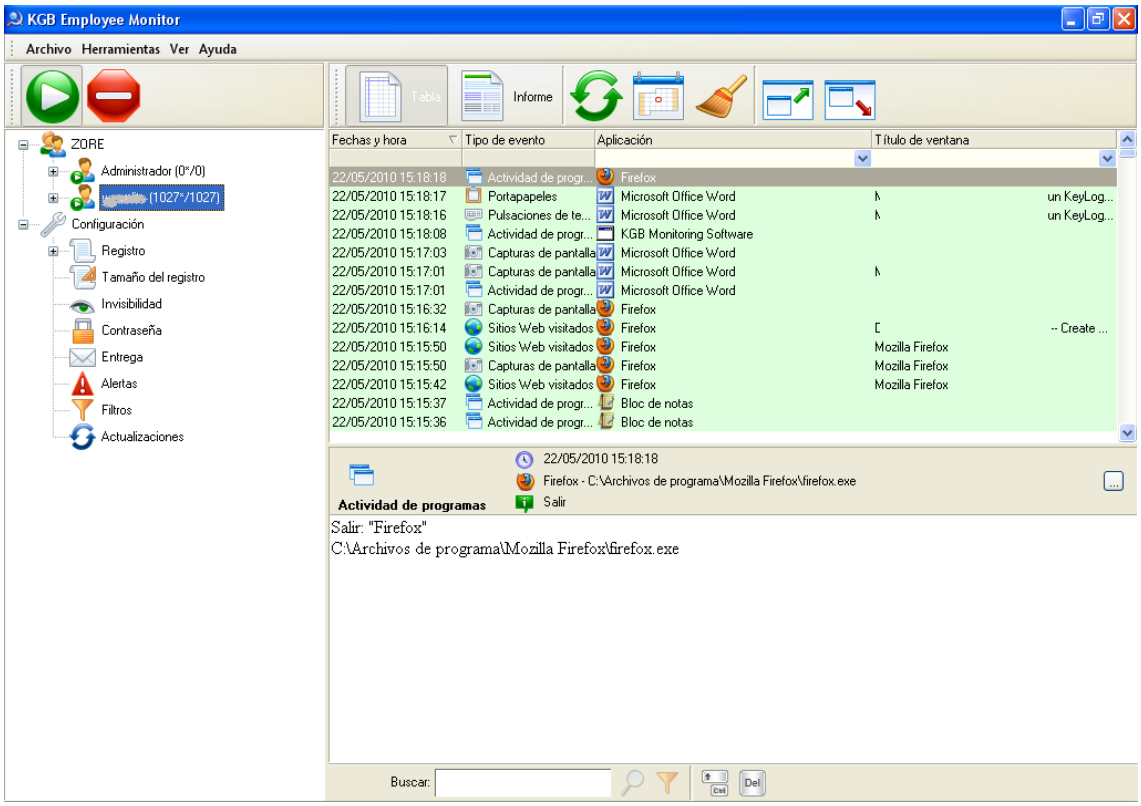
Y ahora les muestro otro KeyLogger de la familia de Refog, uno que funciona muy bien y se consigue fácilmente online…

KGB Employee Monitor

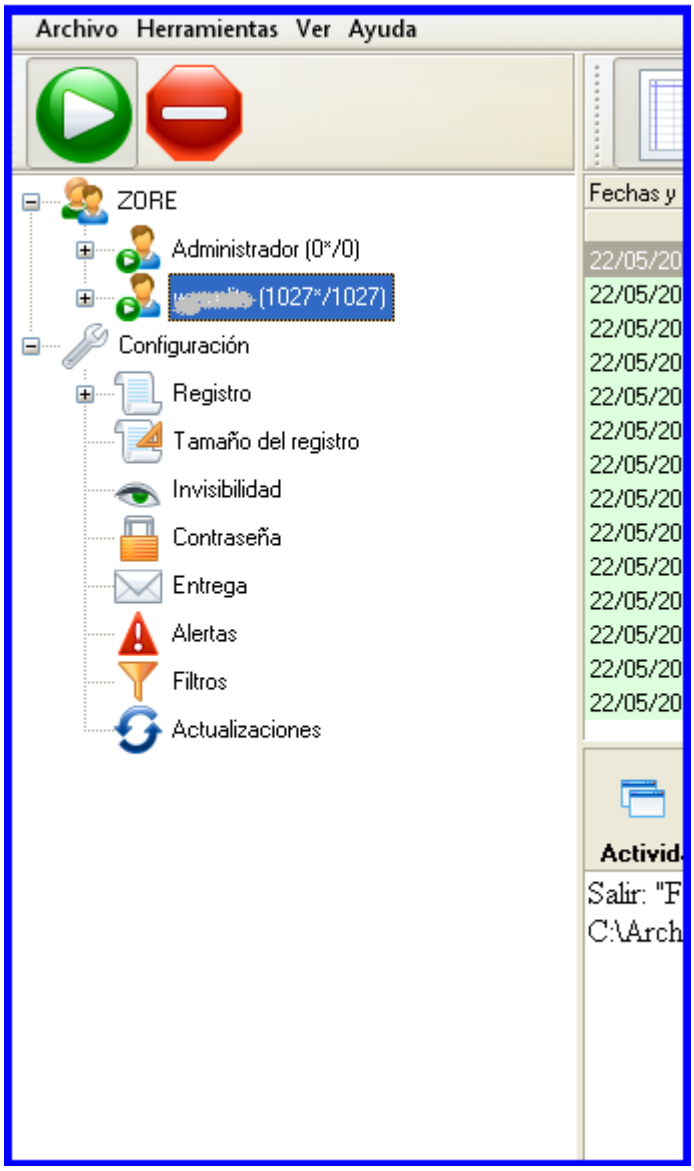


Es el KeyLogger que utilizo y con el que aprendí a utilizar este tipo de software.

Y como vemos en el siguiente screenshot, es casi igual al Refog Employee Monitor…



Es igual, salvo que la parte de configuración está en el mismo cuadrante y árbol que la parte de seleccionar el usuario.



Pero bien, ya finalizando el manual sepan que estas herramientas están al alcance de todos, hay mucho prejuicio en contra de este tipo de software, yo lo veo mas bien como otra opción para ayudar a los demás sistemas de seguridad que seguramente ya estemos utilizando.

No olvides la gran utilidad del Teclado Virtual y prevení que te roben contraseñas.

Suerte con tu KeyLogger y cuidado que si se le da una erróneo o dañino uso se puede volver en nuestra contra, pensalo.

Autor del manual; Damián G. Lasso.
Titular de derechos de propiedad intelectual; Damián G. Lasso.
Contacto con el autor; djlasso@yahoo.com.ar
Mar del Plata, Buenos Aires, Argentina 22/05/2010