Logmein como Troyano

Hector Alejandro Parada Blanco

Descripción

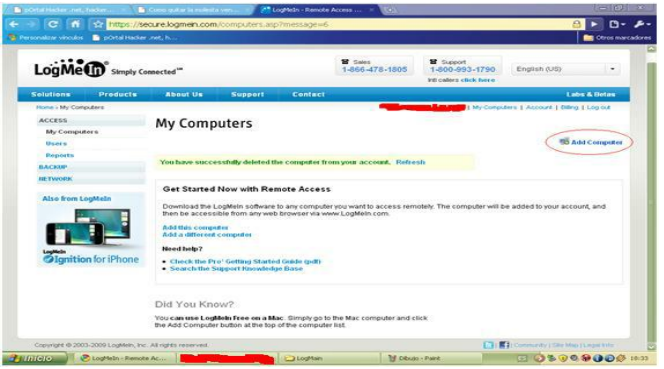
Bueno, he leído algunos post sobre como eliminar los mensajes de conexión remota de Logmein (si, los mismos mensajes fastidiosos que nos delatan), dichos post hablan de modificar una de las bibliotecas de Logmein, contenidas en la carpeta ***X86*** del mismo, pero no explican muy bien el funcionamiento de las mismas, además el Logmein que modifican es una versión ya viejita☺.

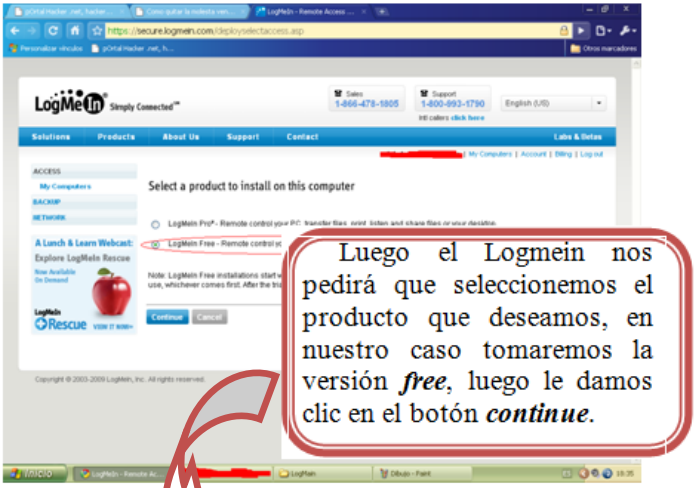
Les mostrare como modificar la ultima versión de Logmein, además de explicar que sucede si eliminamos el recurso o borran el contenido del recurso.

Pasos

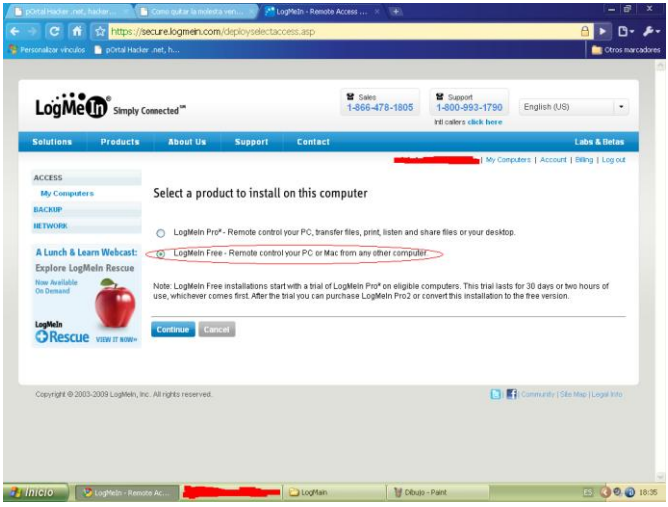
Paso 1 - Lo primero será crear una cuenta en Logmein, desde la siguiente URL: ***https://secure.logmein.com/ES/home.aspx***

Paso 2 – Bien, cuando ya tengamos nuestra cuenta creada, debemos entrar en el computador del cual queremos tomar control remoto. Ingresamos a nuestra cuenta, y le damos clic en el link de ***Add computer***.

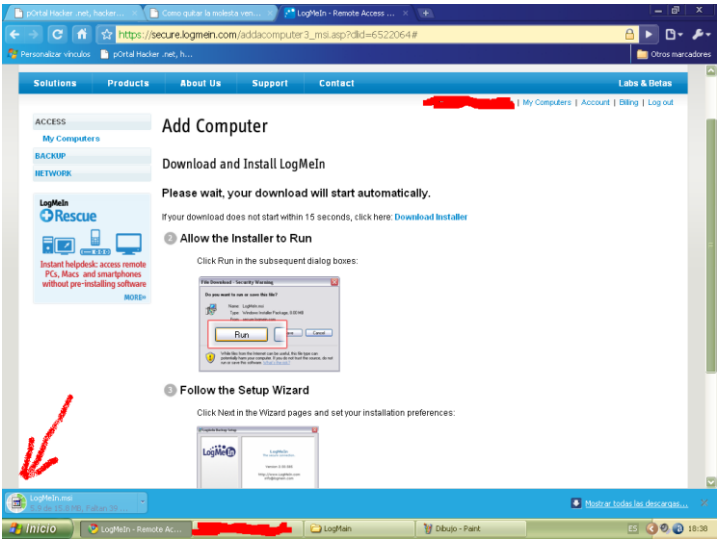




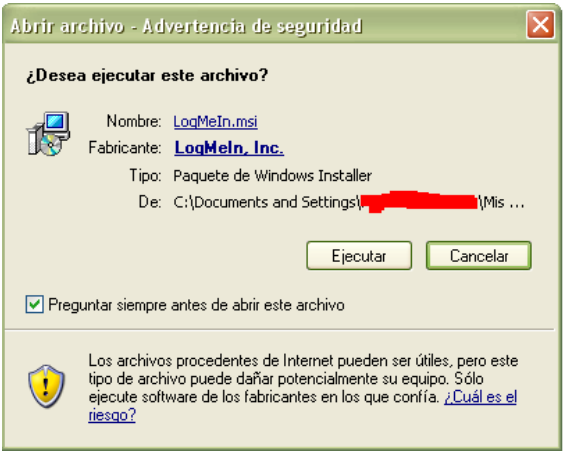
Luego el Logmein nos pedirá que seleccionemos el producto que deseamos, en nuestro caso tomaremos la versión ***free***, luego le damos clic en el botón ***continue***.



Paso 3 – Ahora debemos instalar el Logmein en el equipo victima.

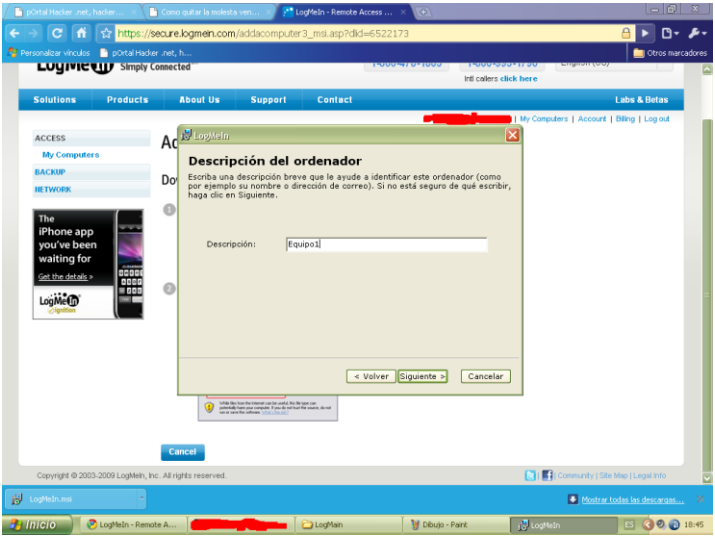


Cuando tengamos descargado el software (tipo agente) de Logmein, lo ejecutamos.

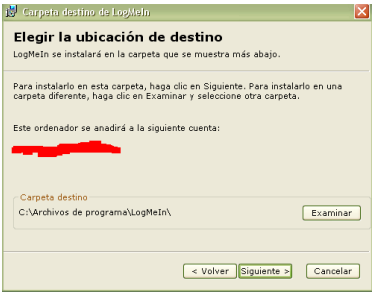


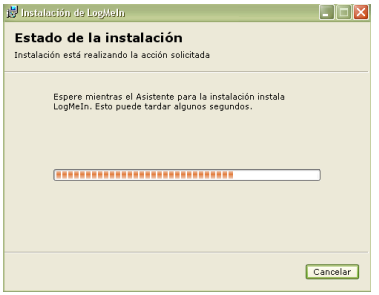
Le damos siguiente y seleccionamos una instalación típica.

Creamos una descripción del equipo o un nombre que lo identifique, este nombre saldrá cuando veamos los ordenadores que tenemos agregados a nuestra cuenta.



Ahora, nos muestra donde queremos guardar el Logmein, dejamos todo como esta y damos clic en siguiente.

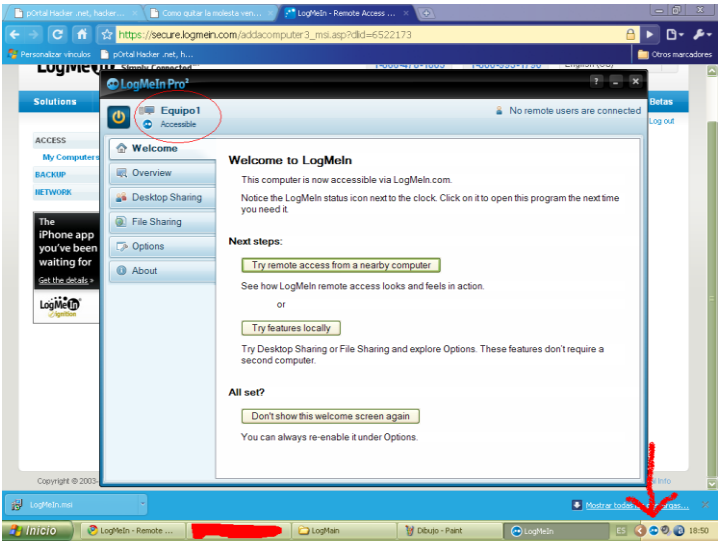




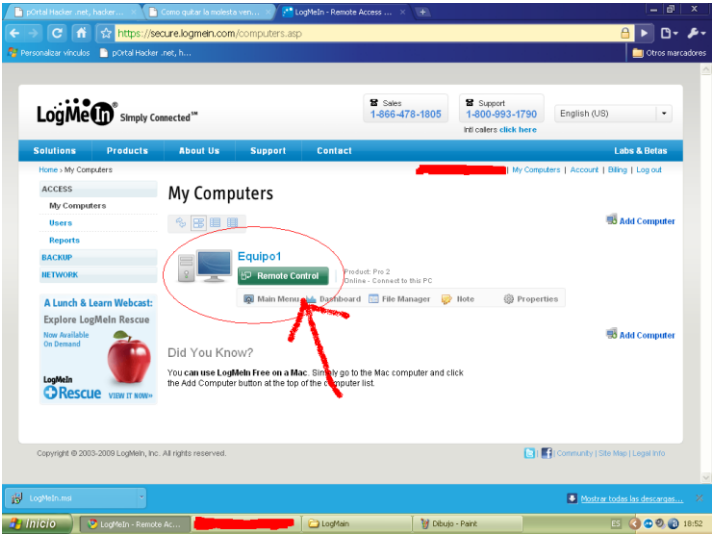
Paso 4 – En la siguiente imagen se puede apreciar uno de los iconos que debemos eliminar para que no nos detecten, el cual

indico con la flecha, además, como se puede ver, tenemos la pantalla del estado de nuestro equipo victima, desde esta ventana podemos cerrar o iniciar la sesión.

Sólo cerramos esta pantalla, sin hacer nada más.



Ahora abrimos nuestra sesión en Logmein, y ya podemos ver los equipos que podemos controlar.



Ahora, le damos clic en el botón de ***Remote control***, luego el logmein nos pedirá el nombre de usuario y la contraseña del equipo victima, para poder iniciar la sesión. Una forma de saber estos datos, es ingresando al regedit, y visualizar el contenido de las siguientes llaves:

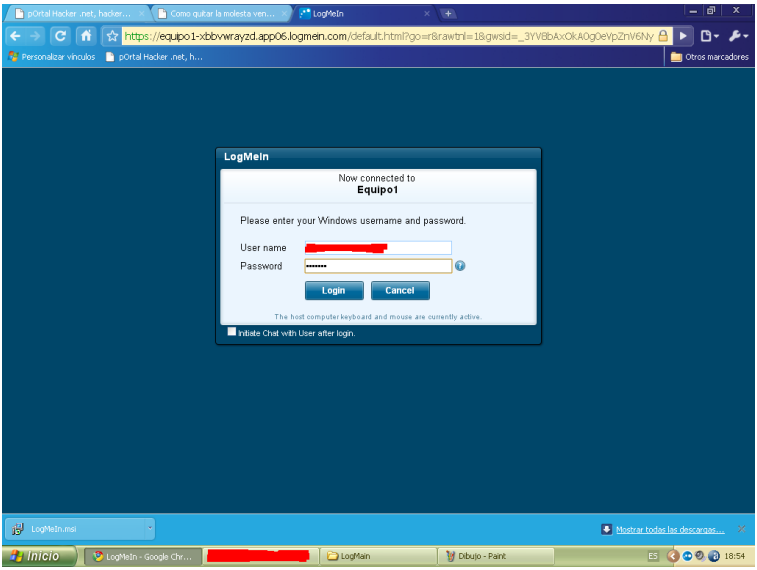
- Guarda el nombre del equipo:

HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/DefaultUserName

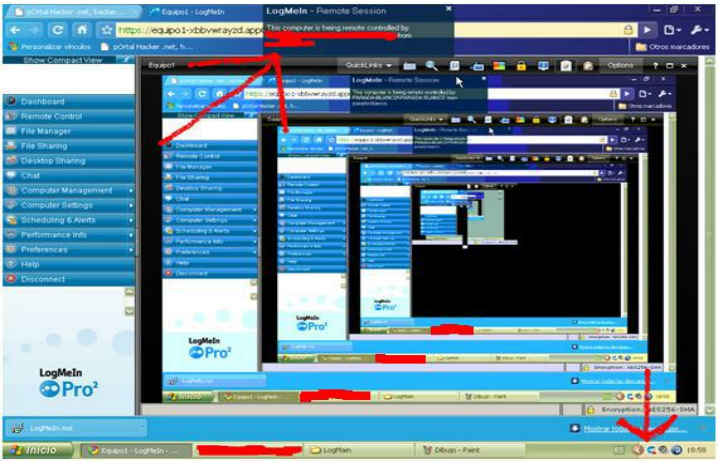
- Guarda el password del equipo:

HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/DefaultPassword

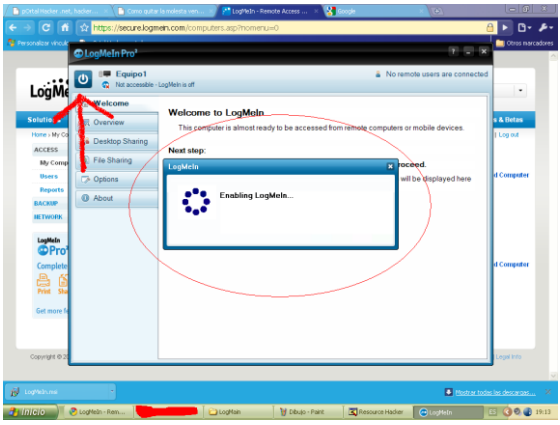
Cuando ya tengamos esta información, la ingresamos y damos clic en ***Login***.



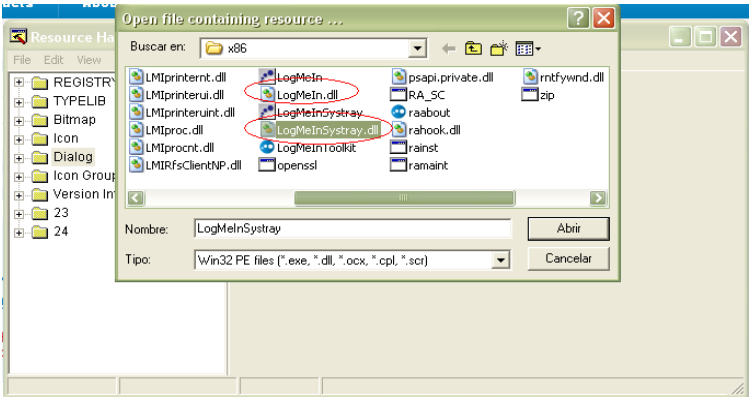
Bien, contamos con el control del PC victima, pero no hemos modificado el software (agente) de Logmein. Como podemos apreciar en la siguiente imagen, hay dos componentes importantes que nos delatan, el primero, ubicado en la parte superior de la pantalla, es un formulario de tipo ***Dialog***, que aparece cuando nos conectamos a el equipo remoto, mostrándole a la victima, quien esta tomando el control del equipo, además, en la parte inferior de la imagen, podemos ver que al lado del reloj aparece el icono de Logmein.



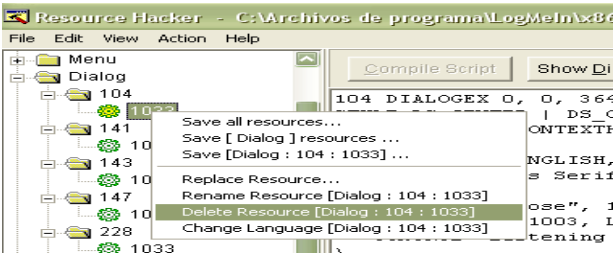
Para solucionar este problema, debemos modificar dos de las bibliotecas de Logmein, para que ni el icono ni el cuadro de dialogo aparezcan más. Pero primero, debemos cerrar sesión, luego abrir el software de Logmein, y le damos clic en el botón de cerrar sesión, para cerrar por completo el Logmein.



Paso 5 – Utilizaremos el software ***Resourse Hacker*** (***ResHack***). Cuando lo tengamos, lo ejecutamos, le damos clic en ***File***, luego en ***Open***, y buscamos la carpeta donde se guardo el Logmein (por defecto se ha guardado en: ***C:\Archivos de programa\LogMeIn***), cuando la encontremos, ingresamos a la carpeta ***X86***, en la cual se encuentran las dos bibliotecas que modificaremos, la primera se llama: ***LogMein.dll***, y la segunda: ***LogMeInSystray.dll***, como se muestra en la siguiente imagen.

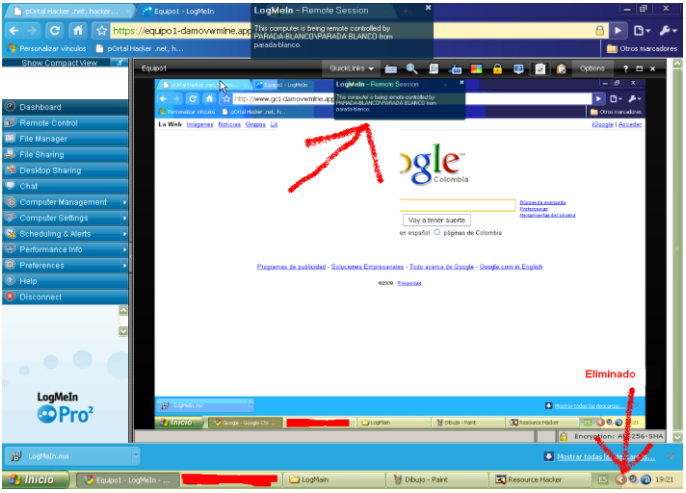


Buen, ahora abrimos la biblioteca ***LogMeInSystray.dll***, nos dirigimos a la rama ***Dialog***, y eliminamos todos sus recursos (104, 141, 143, 147, 228, 229 y 233).

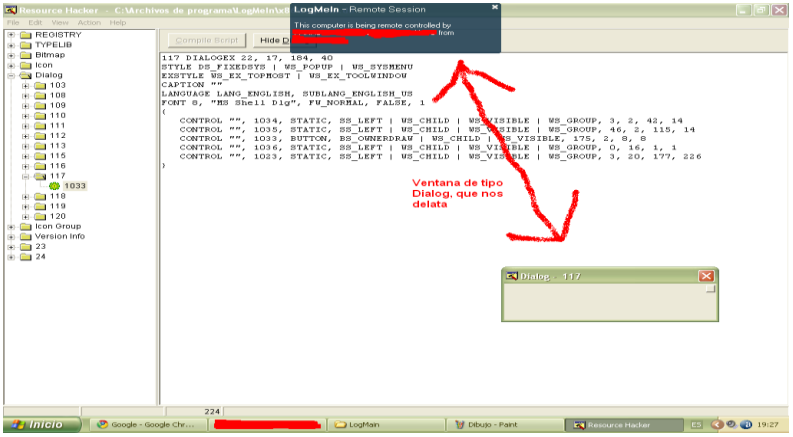


Estos recursos que hemos eliminado, eran las responsables del icono al lado del reloj. Ahora guardamos los cambios.

Ejecutamos el software de Logmein e iniciamos sesión de nuevo, tomando el control del equipo, como podemos ver, el icono molesto al lado del reloj desapareció, pero aun nos falta el cuadro de dialogo.

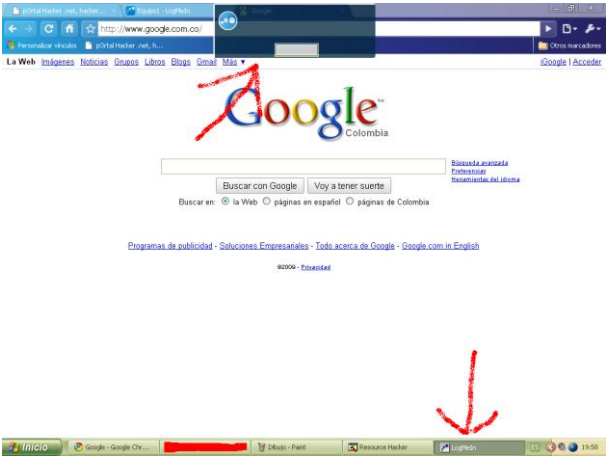


Cerramos de nuevo sesión y detenemos el programa de Logmein, luego abrimos el ***ResHack***, vamos a ***File***, ***Open***, y abrimos la biblioteca que nos falta: ***LogMein.dll***; Ahora bien, nos dirigimos a la rama ***Dialog***, y no vamos al recurso 117, como podemos ver en la siguiente imagen, este recurso crea el cuadro de dialogo que nos delata.

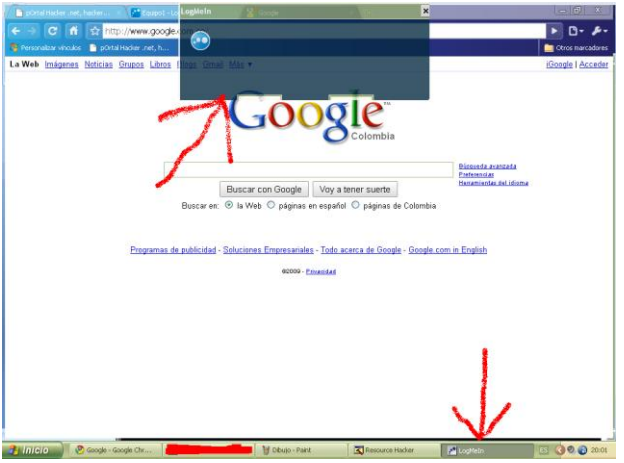


Debemos eliminar este recurso, pero, si solo eliminamos este recurso, en ocasiones (no siempre☺) el logmein busca otros recursos que remplacen al recurso eliminado, veamos como funciona. Si iniciamos sesión e iniciamos el software de Logmein en el equipo victima con los cambios que hemos realizado, podemos ver que el Logmein a buscado el recurso 118 de la rama ***Dialog*** y si este recurso es eliminado el Logmein buscara el recurso 119, pero si este recurso no esta, el Logmein buscara el recurso 120, por eso, debemos eliminar también los recursos 118, 119 y 120.

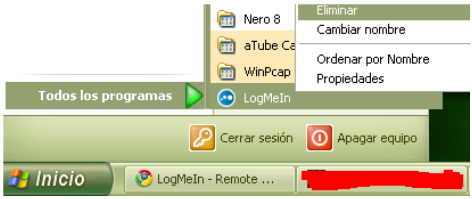
- Recurso 118: si eliminamos sólo el 117



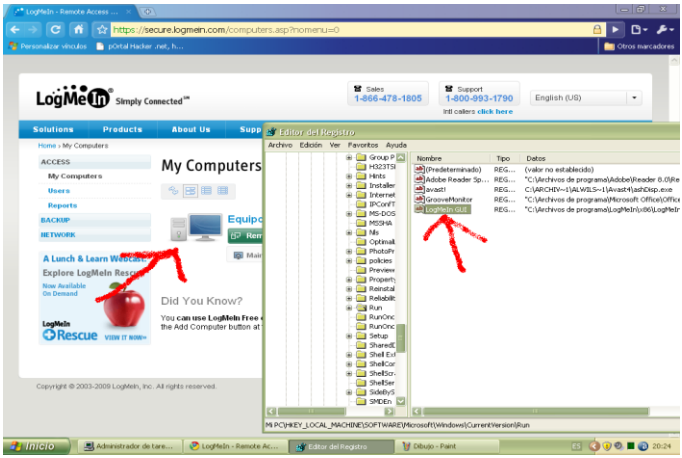
- Recurso 119: si eliminamos el 117 y 118.



Bueno, una vez eliminados dichos recursos de las dos bibliotecas antes mencionadas, debemos eliminar el Logmein de la vista de ***Todos los programas***.



Nota: no es necesario, modificar el registro de ***Windows***, para que el Logmein se active cada vez que inicia el sistema, ya que por defecto el Logmein se ha guardado en el registro y se iniciara cada vez que el PC es reiniciado.



Y fue todo, ya el usuario del equipo victima no se percatara cuando ingresemos remotamente por medio de Logmein.