¿Los Antivirus realmente nos protegen?

By 4n0nym0us

Eliminando un Spy de nuestro sistema

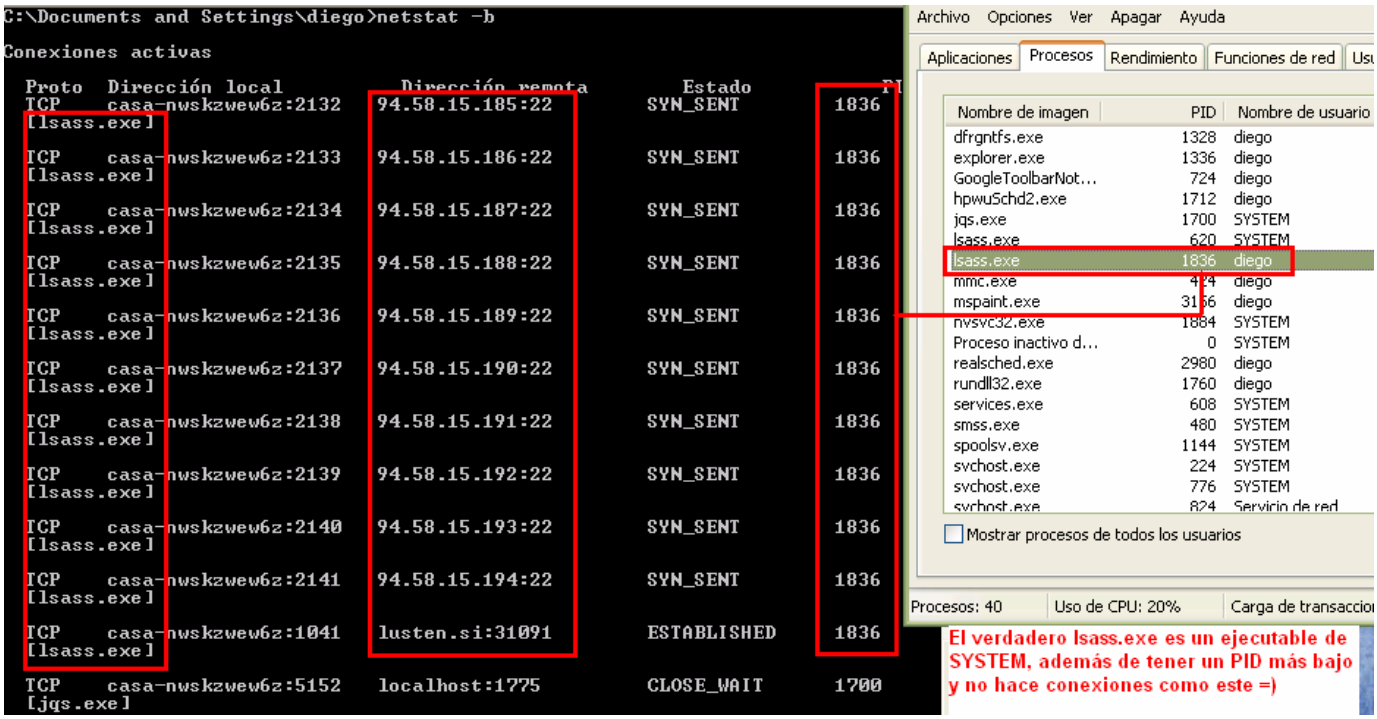
Este documento está creado didácticamente para no solo mostrar las vulnerabilidades de 39 de los mejores antivirus del mercado, si no también para enseñar de una forma clara y entendible como encontrar y eliminar algunos tipos de malwares de nuestro sistema.

Bueno hace un par de días un compañero de trabajo me vino alarmado con su PC ya que este de repente empezaba a tener una conexión demasiado lenta al conectarse a Internet y el equipo en sí, además le consumía un 90% de la memoria disponible.

Estaba casi de claro que le entro un virus, lo cual lo primero que hice fue mirar el administrador en busca de algún proceso extraño…

Me llamo la atención el encontrarme con un **lsass.exe** con su nombre de usuario cargado en memoria, ya que el original se carga de sistema…

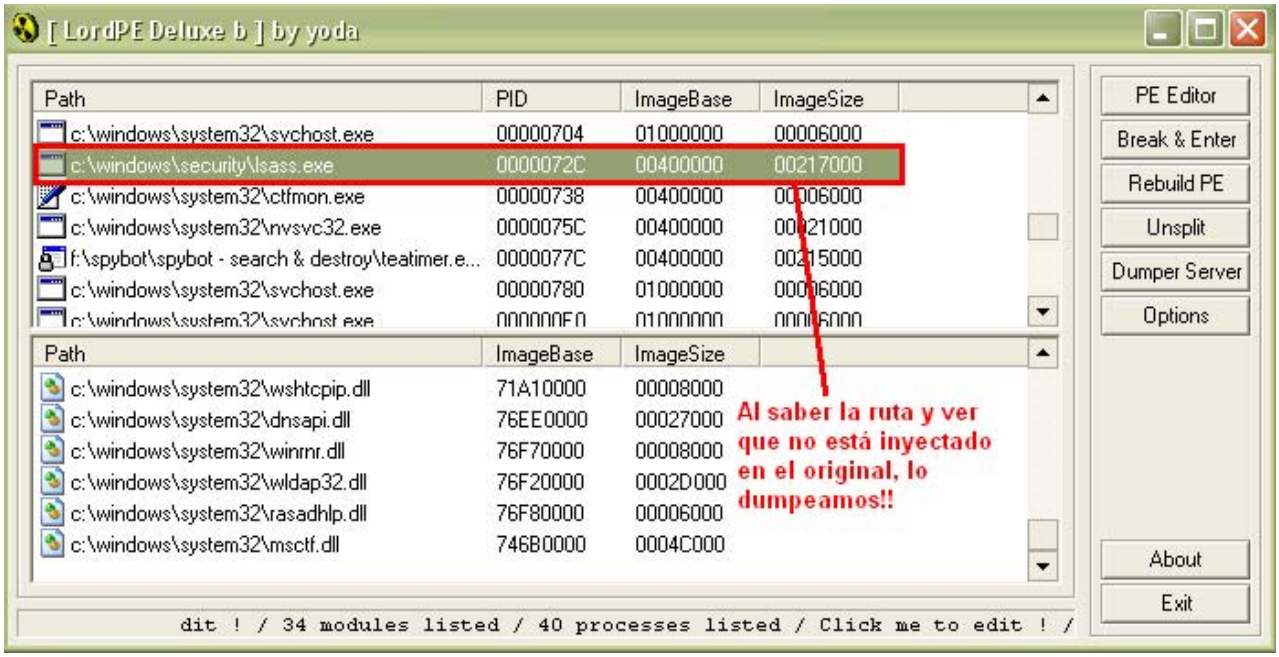
Rápidamente fui a consola he hice un **netstat –b** para ver los procesos y sus conexiones, impresionantemente había un montón de incesantes intentos de conexión desde dicho proceso al mismo rango de IP únicamente se le sumaba uno a la última cifra… parecía estar hecho para petar mi red…



Abrí mi querido **LordPE** para buscar el **PID,** este en Hexadecimal ahora por si estaba inyectado en el verdadero **lsass.exe** y escondía la ruta original…

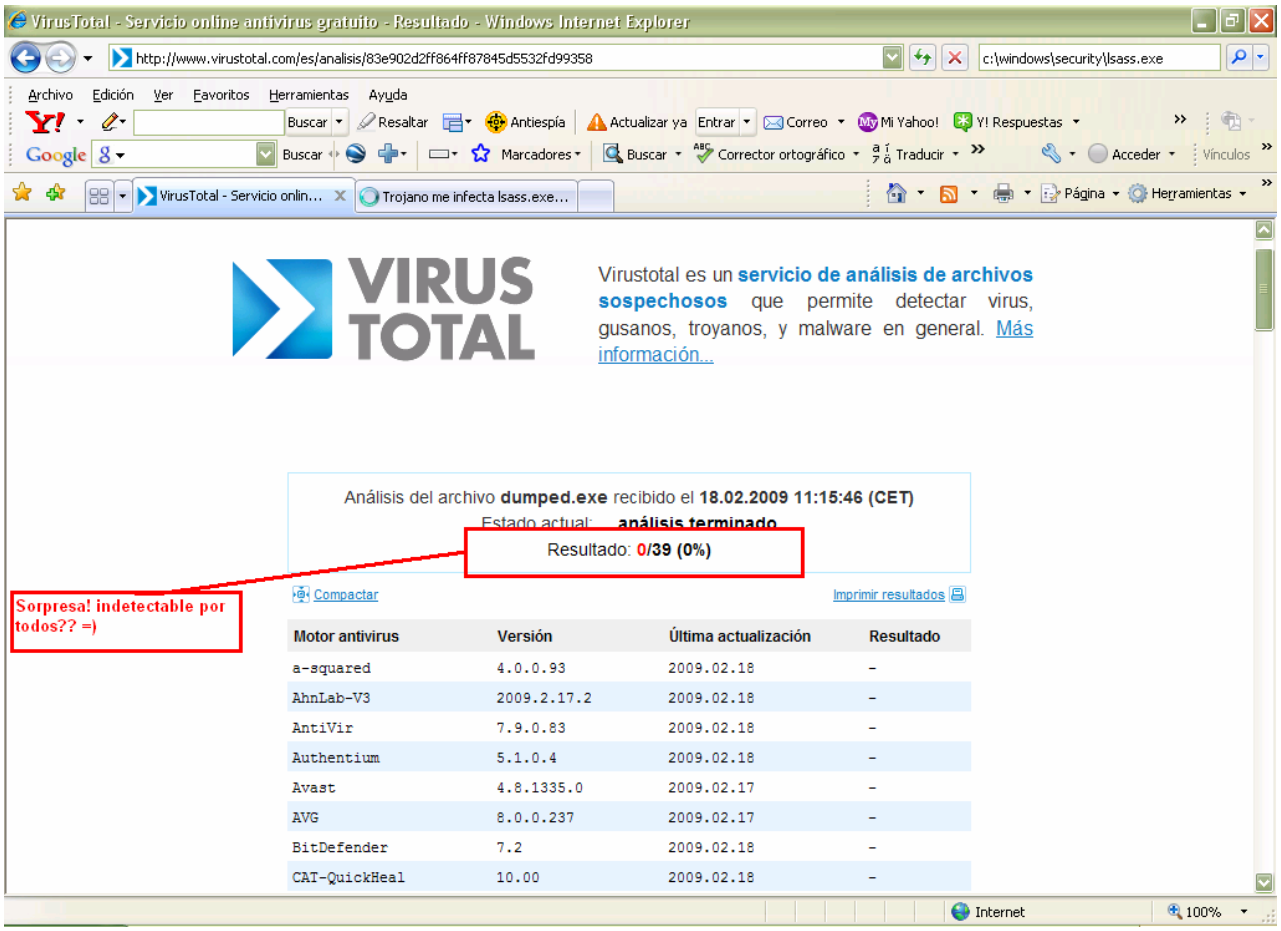
1836 = 72C

Nos dirigimos a este **PID** desde el **LordPe** y nos encontramos con que la ruta del falso **lsass.exe** es otra totalmente distinta de la original, ya que el de Microsoft se aloja de forma predeterminada en la carpeta **"C:/Windows/System32"** y este misteriosamente lo hacia en **"C:/Windows/Security":**



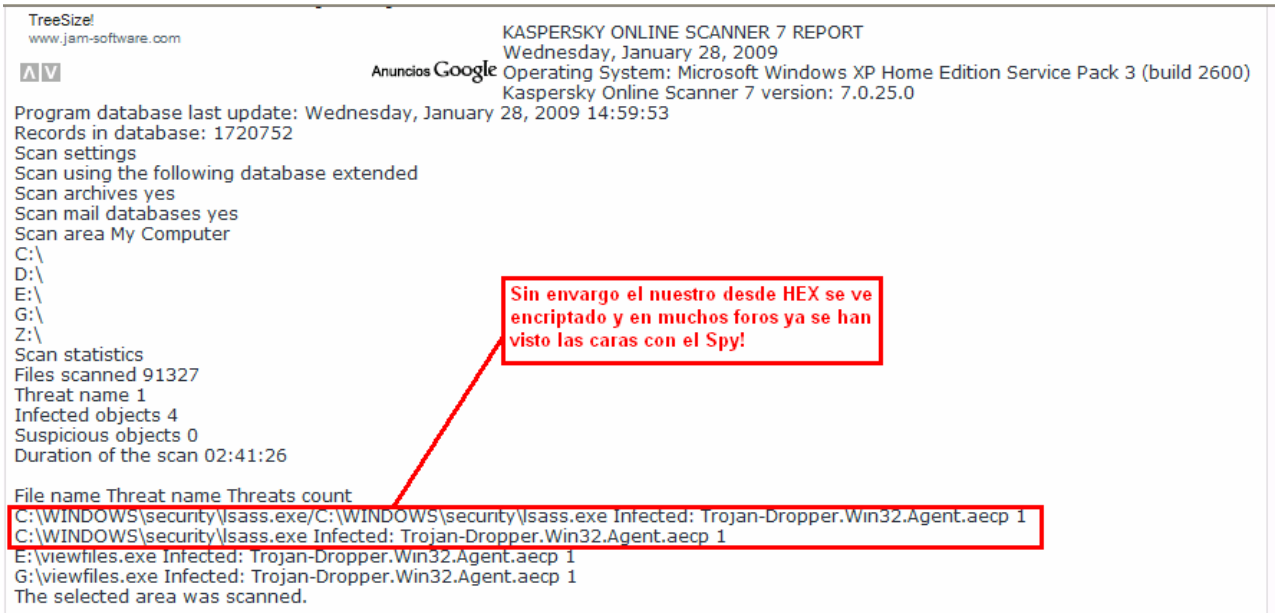
Pinchamos con el botón derecho y hacemos un **Dump Full** para copiar el archivo que funciona en memoria y tenerlo más a mano…

Una vez dumpeado se guarda en el escritorio y fue enviado a un Scanner Online con **39 Antivirus**, veamos el resultado del Scanner…



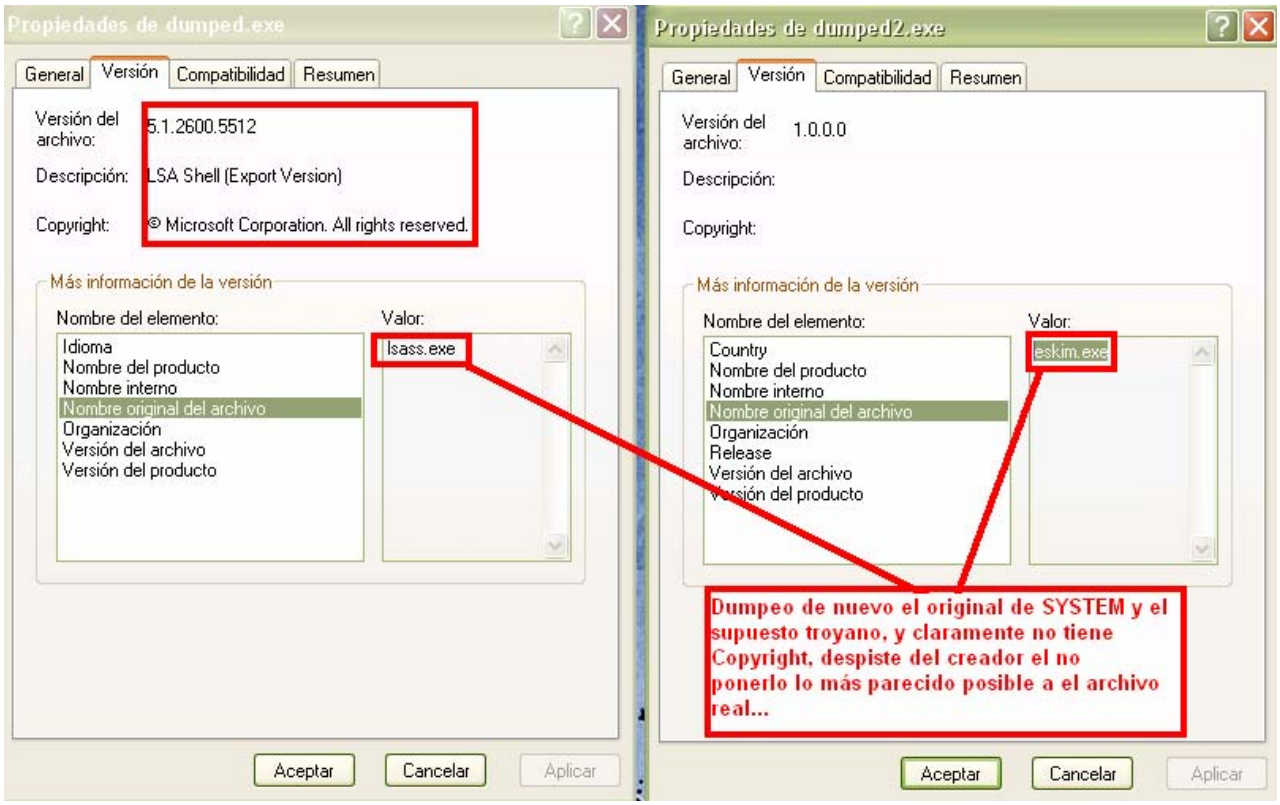
Algo no cuadra, es seguro que este archivo está infectado y los Scanners no nos alarman... sigamos con la investigación.

Bueno lo siguiente que hice fue poner la ruta de **“C:/Windows/Security/lsass.exe”,** y bien encontré mucha información sobre varios foros que alarmaban de un muy posible malware escondido en esa carpeta, aunque en estos los antivirus si lo detectaban…

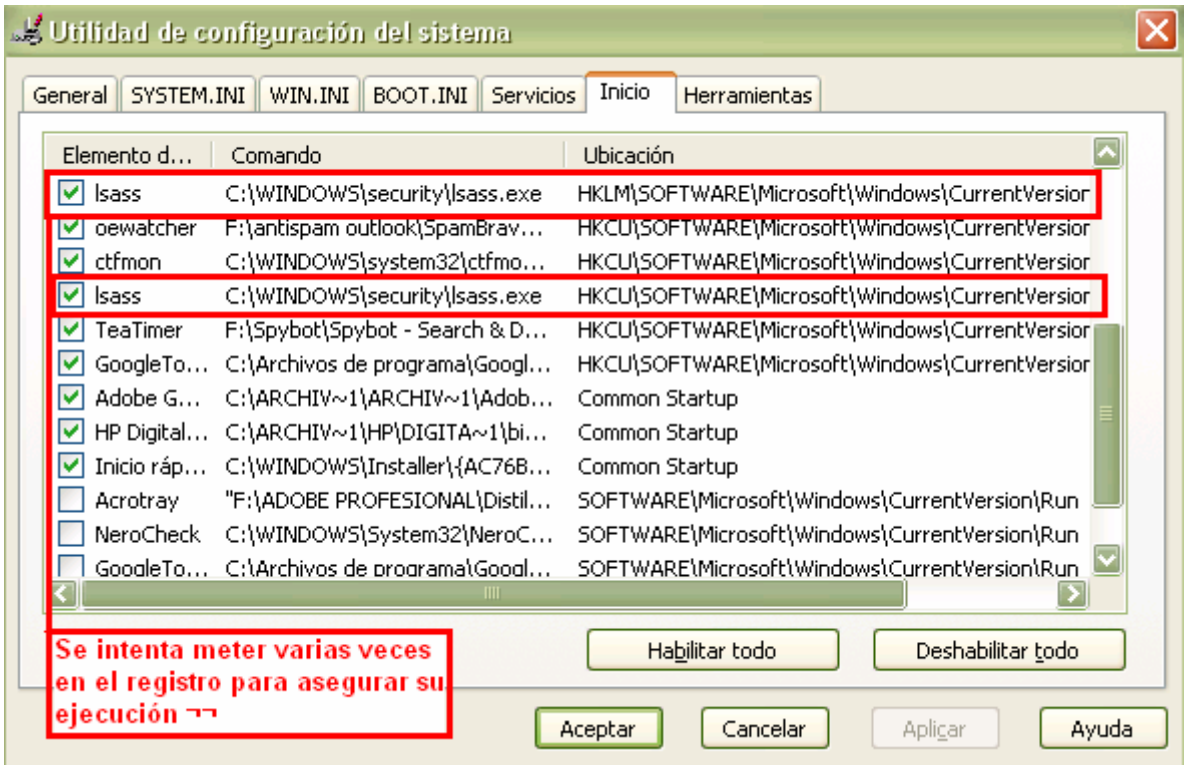


Desde Hexadecimal el archivo parecía totalmente encriptado así que supuse que era muy posible que fuera este el motivo de ninguna alarma.

Me dispuse a dumpear ahora los dos archivos el **lsass** de la carpeta original y el sospechoso, claramente como se ve en la imagen tenían claras diferencias en sus versiones, en peso y código…



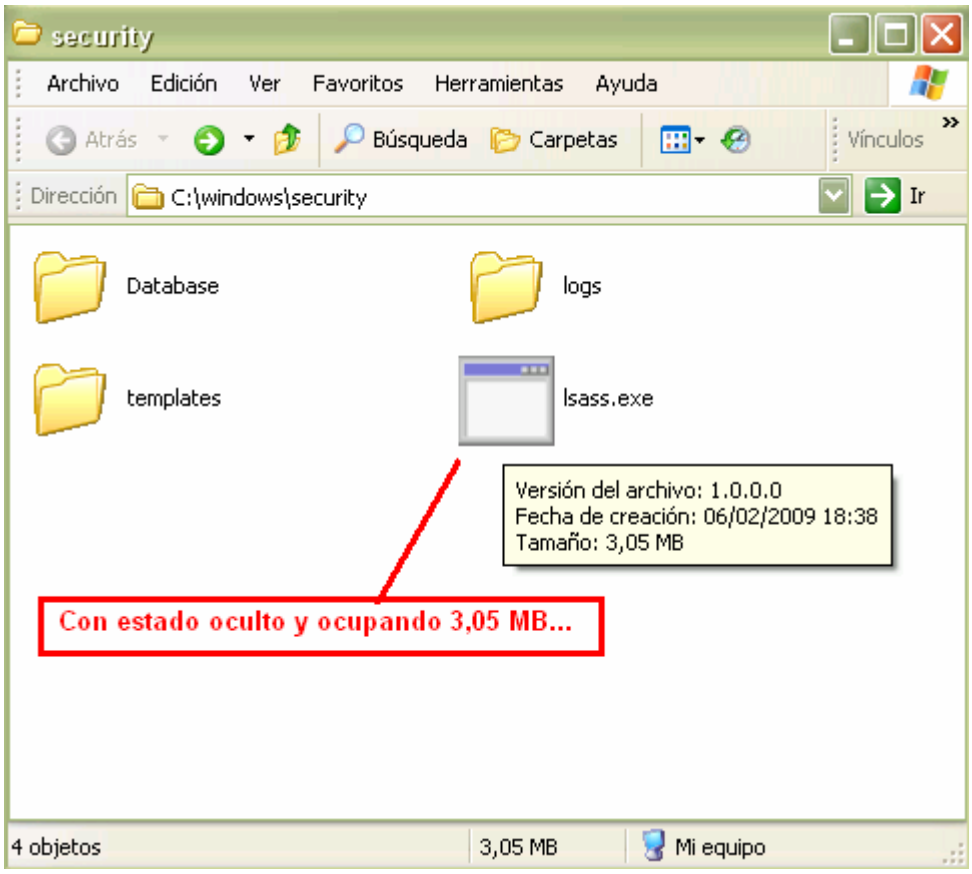
Después de salir de tantas dudas ante si en realidad era un malware me parecía bueno ver de que forma se lanzaba en el sistema para iniciarse automáticamente, así que me dirigí a **msconfig** desde ejecutar:



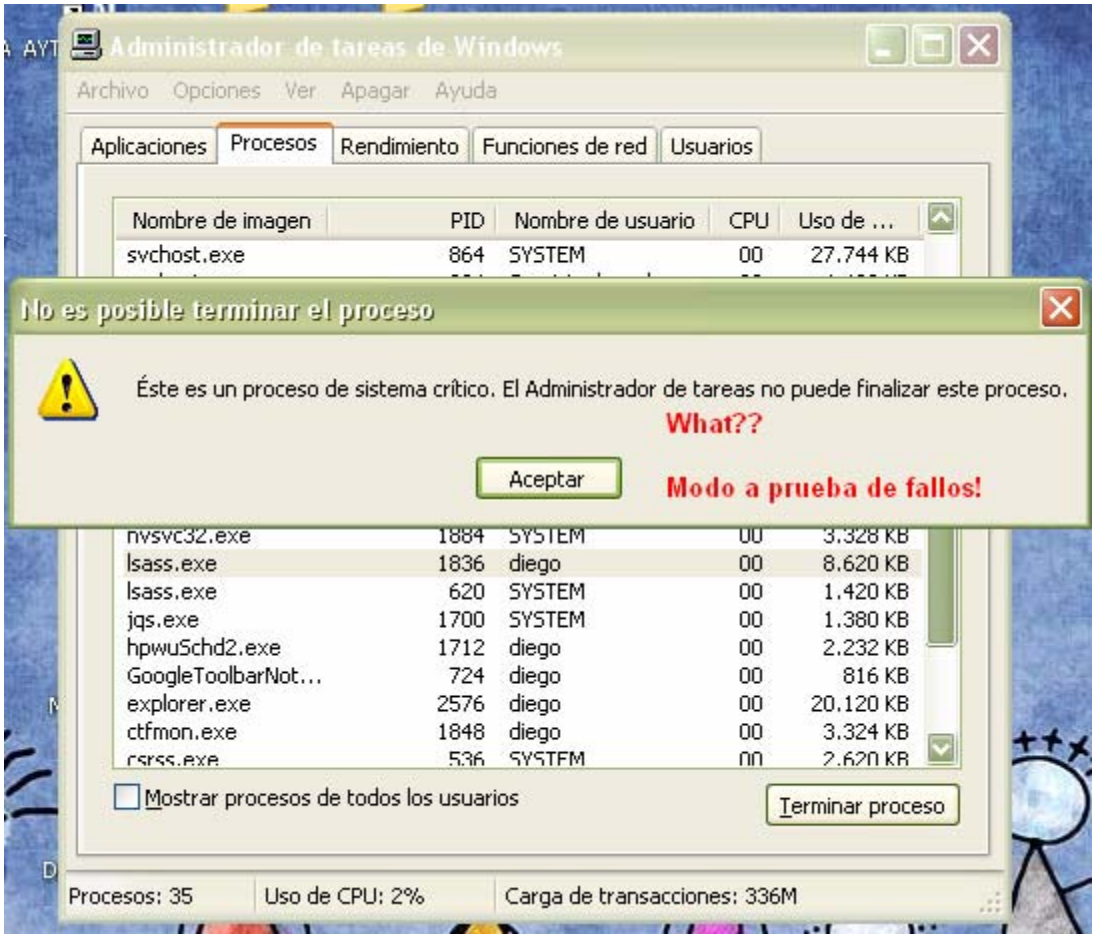
Claramente se veía incluso en el nombre de la entrada que lo intentaba varias veces para asegurarse que el archivo se ejecutaría…

Ahora ya si me decidí entrar en la misteriosa carpeta para identificar de manera visual a mi contrincante xD!!

Observando el archivo vemos que está de forma oculta de solo lectura y pesa 3,05MB, algo bastante raro para ser este archivo el de sistema…



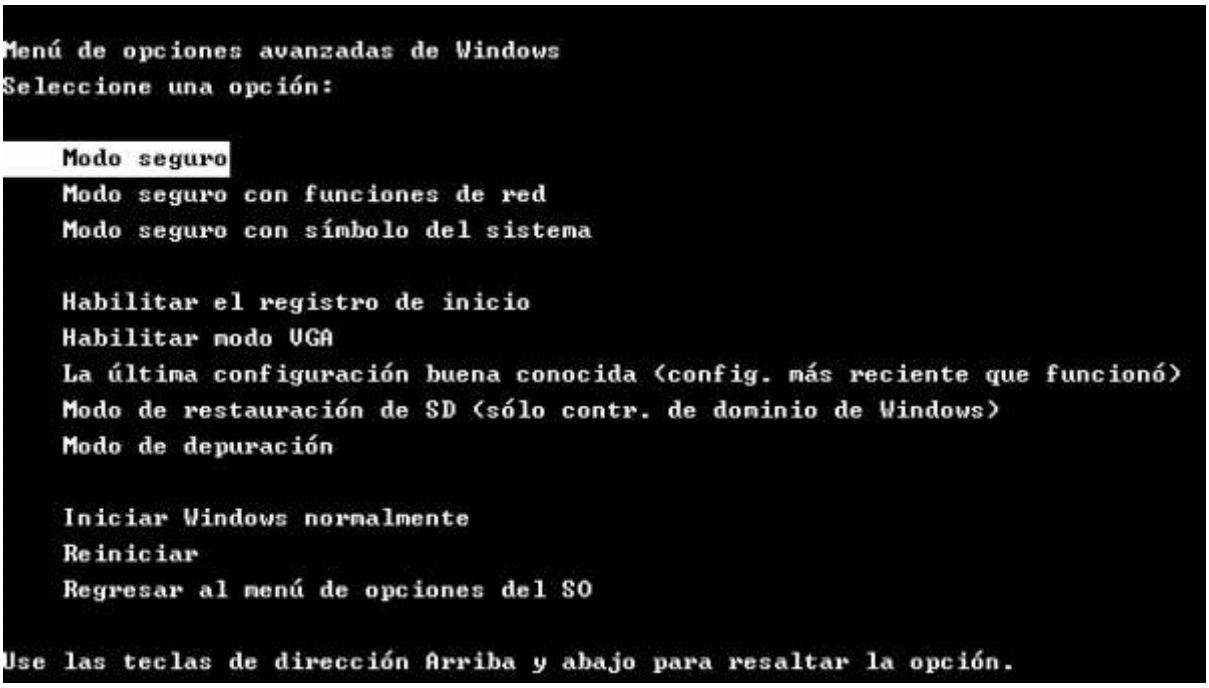
Con un “**Contrl + Alt + Supr”** saco el administrador de tareas para eliminar el proceso de manera fácil y poder eliminarlo manualmente, pero me salta para mi información que es un proceso critico! **¿¿??**



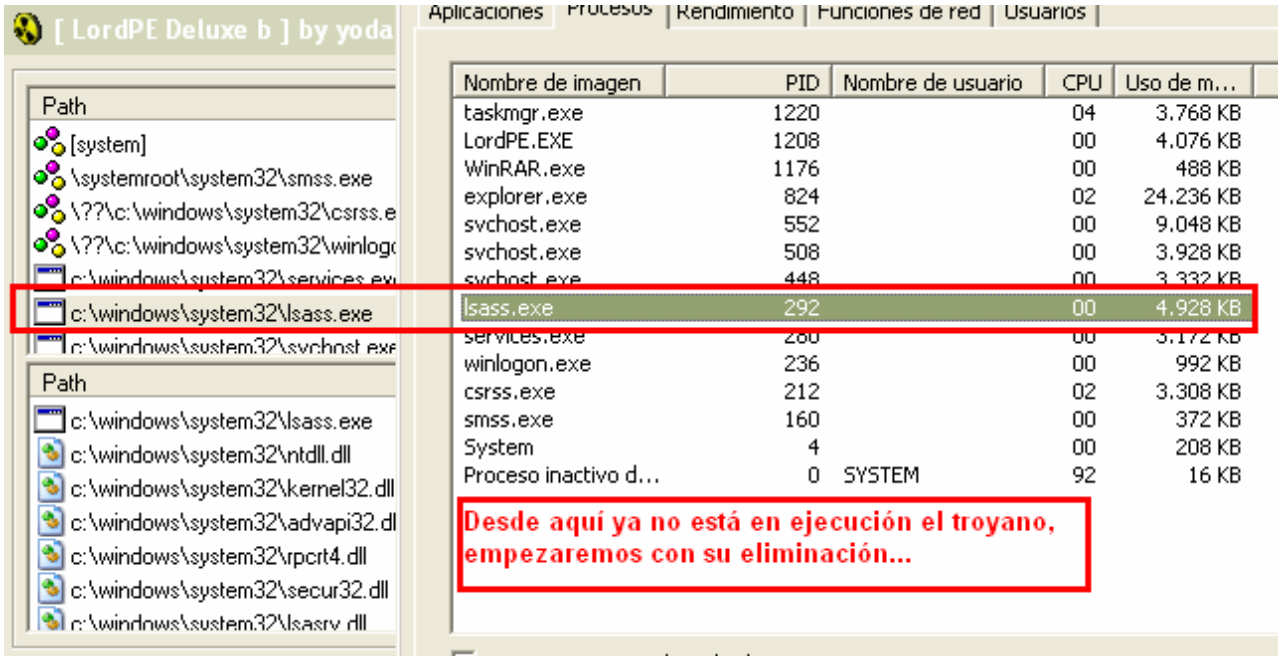
Lo cual corriendo a modo a prueba de fallos para que no se ejecute con el inicio y poder eliminarlo fácilmente.

Nos disponemos a reiniciar la máquina.

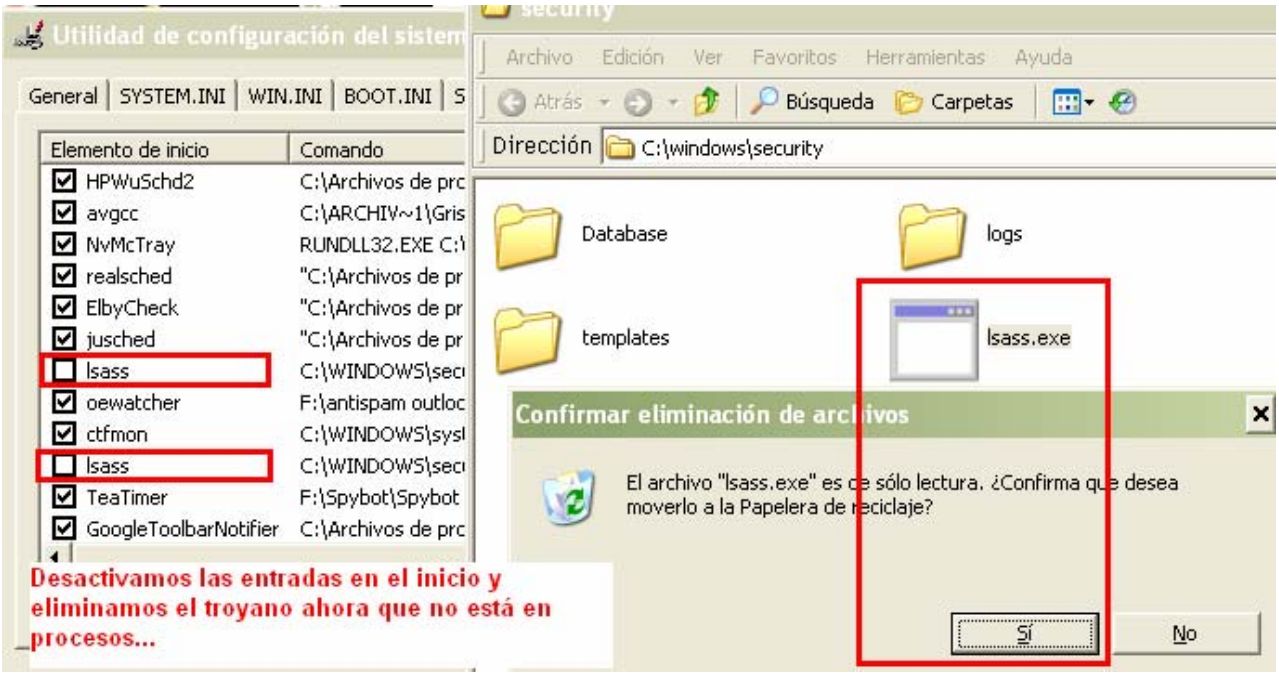
Presionando **F8** antes de la iniciación del sistema para entrar al **Modo seguro**:



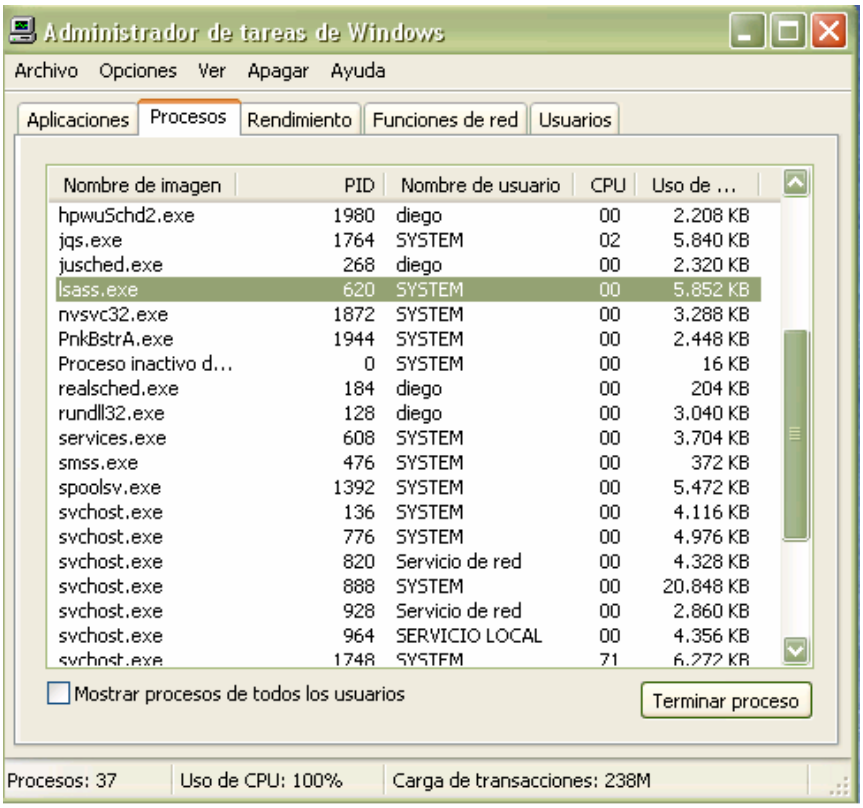
Una vez dentro del sistema saco de nuevo el **LordPE** para contemplar que proceso **lsass.exe** es el que se está ejecutando:



Viendo que el que corre es el original y el otro permanece dormido, vuelvo a las claves de registro y a eliminar el archivo de la carpeta **Security**:



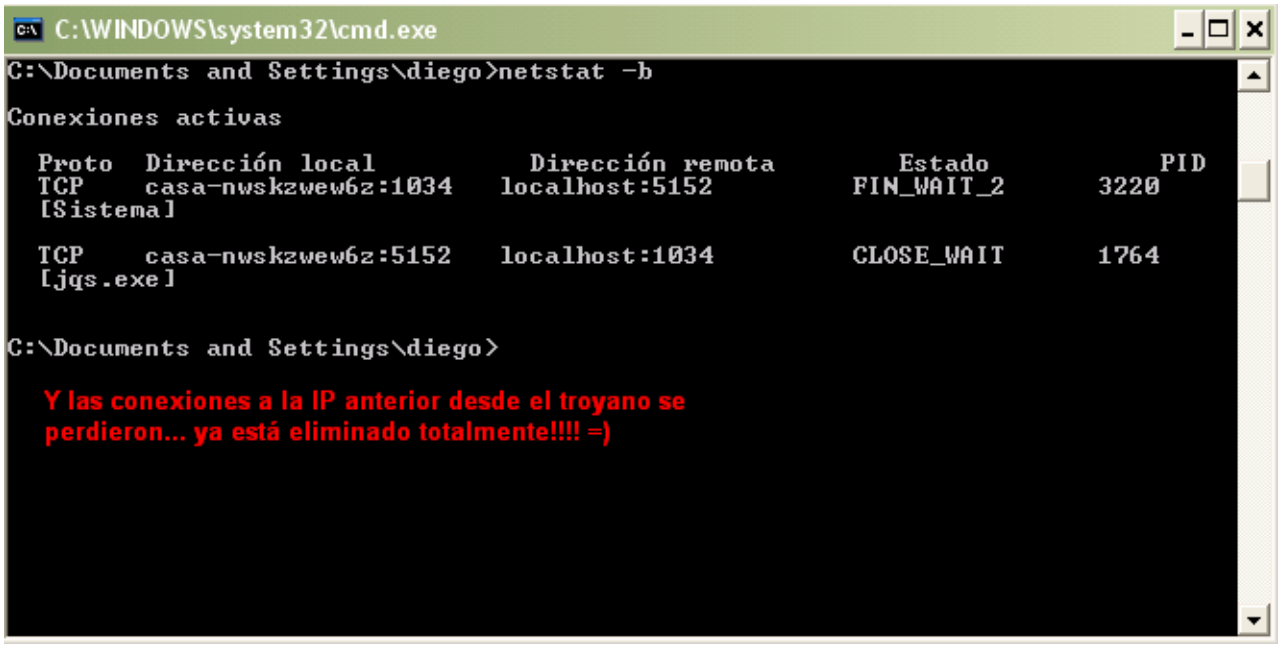
Una vez acabado con este nos disponemos a reiniciar el sistema y entrar en modo normal a la sesión del usuario…



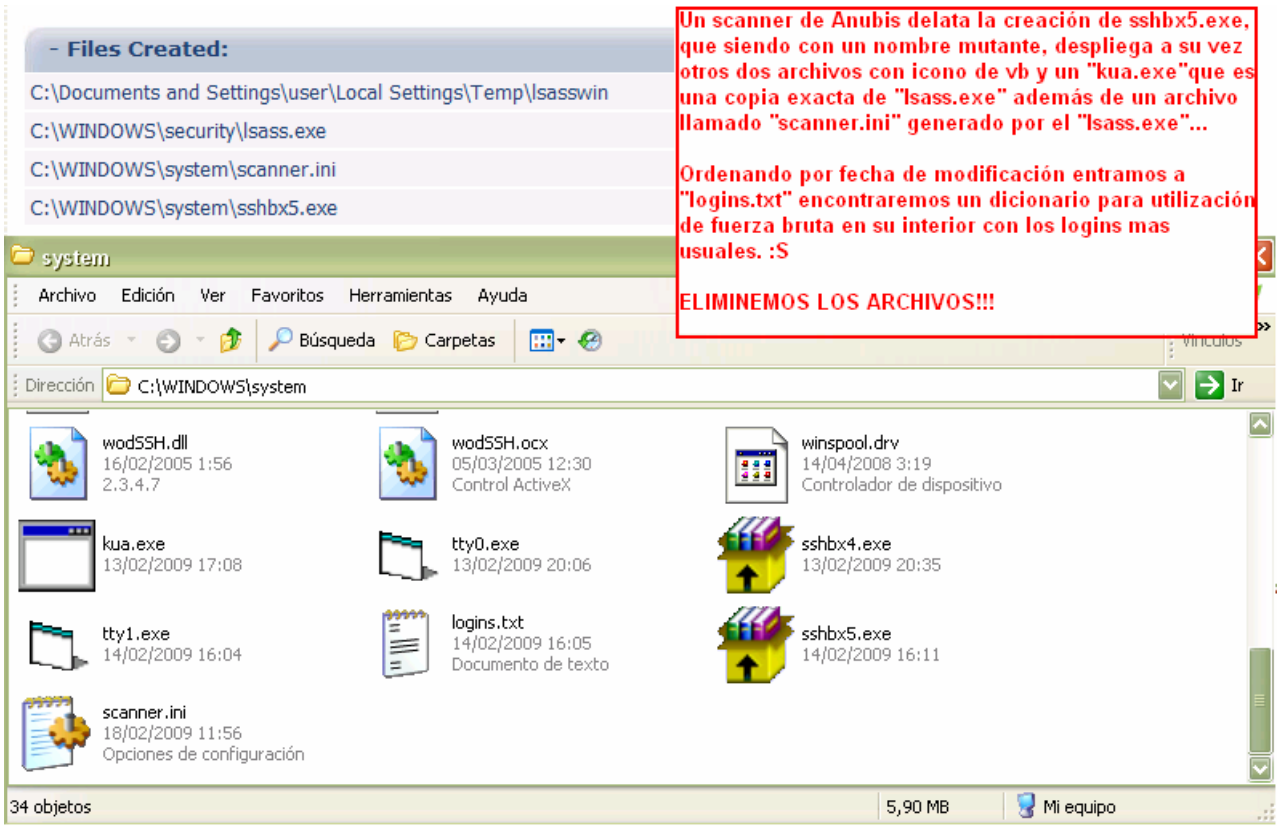
Una vez vueltos al sistema en modo normal vemos que el lssas.exe ha desaparecido, y el funcionamiento del equipo ahora es más rápido =)

Como se ve en la imagen anterior el **lsass.exe** que está corriendo ahora es el de sistema.

Volvemos a consola para ver si con un **netstat -b** si muestras las anteriores conexiones:



Intrigado por saber que tipo de malware era envié un Scanner del archivo infectado a Anubis el cual me mostró lo siguiente:



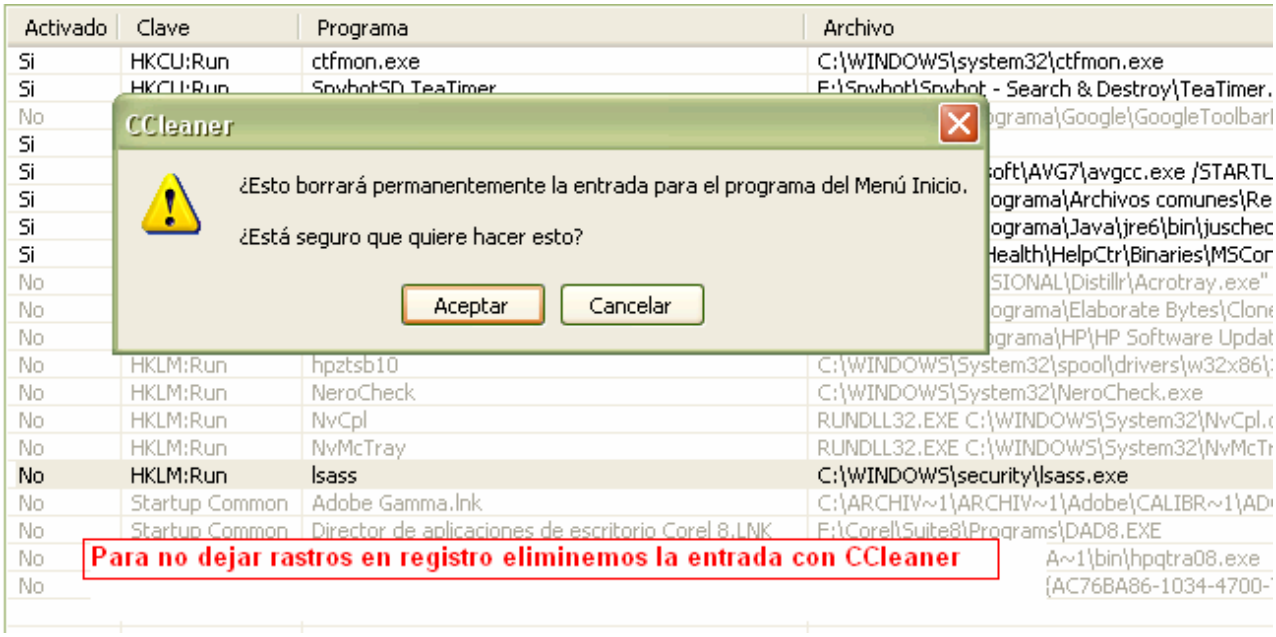
De todos estos archivos el que más me llamo la atención fue el **logins.txt**, ¿Para que quiere un archivo plagado de palabras?

Bien recopilemos información:

Las IP conectadas eran iguales, únicamente variaba su último número de orden siempre seguido, el puerto de conexión utilizado era el **22**, siendo este el de serie para las conexiones desde el protocolo **SSH**, además de crear dos archivos aleatorios llamados "**Ssh**bx?.exe", tenemos un "**logins.txt"** con una burrada de palabras para ataques de diccionarios como **Admin Admin.- Root Root - User User**…

Mi conclusión clara es que nos encontramos con un **Robot**, el controlador nos usa de máquina **Zombie** para realizar ataques fortuitos por "**Ssh"** a todas las direcciones de IP que se encuentre por su paso por ataque de diccionario, cuando una de estas sea acertada se le enviará todo a nuestro pequeño delincuente…

Bueno acabando dejando la indagación ante tanta confusión me despido y termino eliminando los archivos y las claves de registro para que no haya más problemas…



Espero que al menos les haya sido tan entretenido como a mí y de su agrado.

Un Saludo =)

By 4n0nym0us

Para indetectables.net

MSN: 4n0nym0us@Professionalhackers.gov