Se nos viene la clase 51 encima. Cuento que éste es una profundización de lo que veníamos viendo en la introducción. Voy a repetir cosas de allí, no se molesten por favor:D.

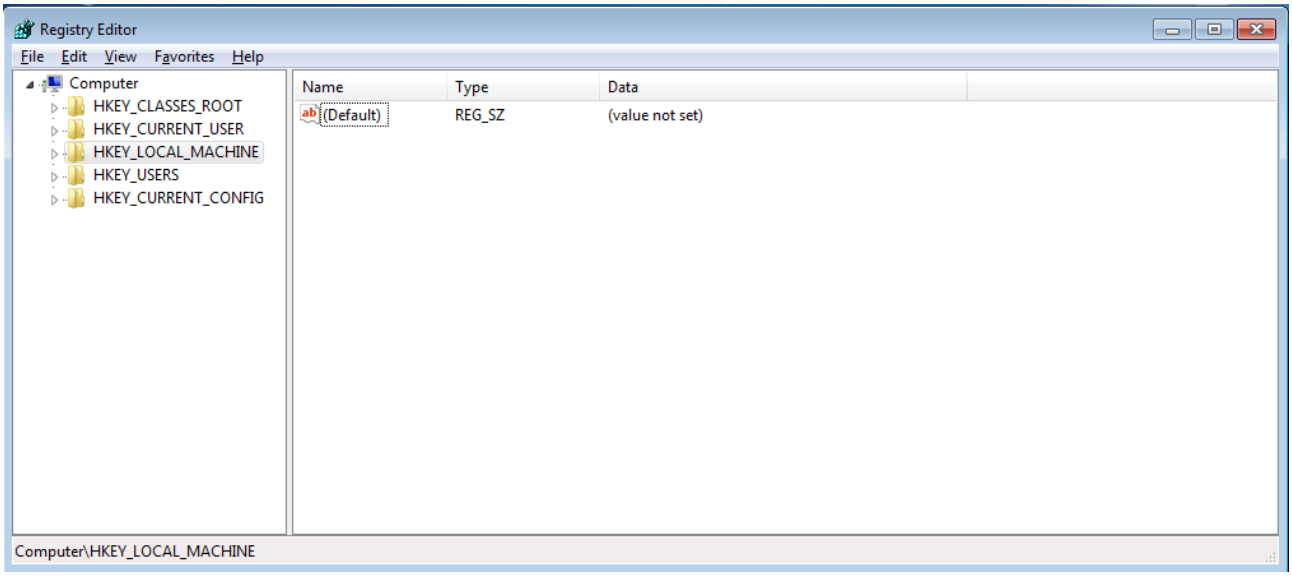
“Yo siempre toqué el registro de Windows para mejorar el rendimiento de mi PC. ¿Qué es éso?”

Bueno, el **registro** de Windows es una **base de datos** que tiene **configuraciones** del sistema operativo y el software instalado. De aquí lee las configuraciones el kernel, los drivers y otros componentes muy importantes del S.O.

“Entonces me imagino que es muy importante.”

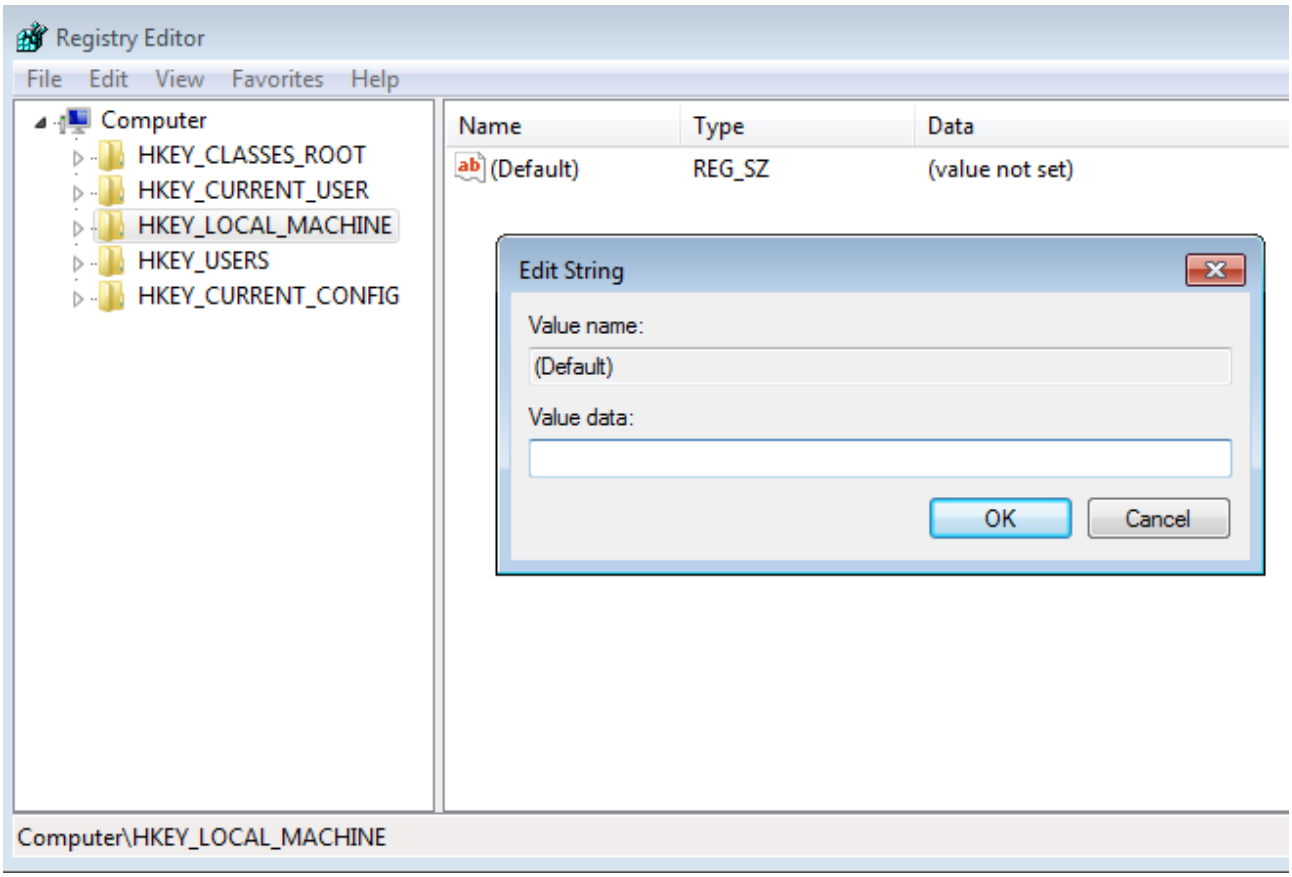
Ni hablar, Manolo. Es realmente una de las **columnas principales** de este sistema. Nosotros podemos cambiar estos valores y que funcione como nosotros queramos. Imaginen que aquí (como un ejemplo fácil) aparecen los programas que inician con el sistema. Si nosotros lo configuramos para que inicie un backdoor que se conecta a nuestra PC cada vez que inicia, vamos a poder tener acceso permanente ;). Pero éso es sólo una pequeñez de la funcionalidad que tiene el registro.

Vamos a ver el **editor del registro**, así puedo enseñarles más prácticamente. Vamos a **Inicio** -> **Ejecutar** (**run** para los que lo tienen en inglés), o tecla **Windows+R**. Escribimos "**regedit**" sin comillas y le damos al Enter. Veremos algo como ésto:



"Entonces tenemos carpetas y archivitos raros."

En realidad son **claves y valores.** Mira Manolo, lo que aparece en la parte de la **derecha** es un **valor**. En este caso es un valor que **contiene** un **texto** -nos podemos guiar por el **ícono** o podemos afirmarlo con el valor en la columna **Type**- pero que no está completado con nada en particular. ¿Podemos editarlo? Claro que sí, vamos a darle doble click.



Entonces aquí tenemos la posibilidad de **darle** un **valor** que nosotros queramos. Cerremos esa ventanita. ¿Ven las **carpetas** que aparecen a la **izquierda**? Bueno aquellas son las denominadas **claves.** Si las abrimos veremos **subclaves,** que a su ves tienen mas valores y subclaves.

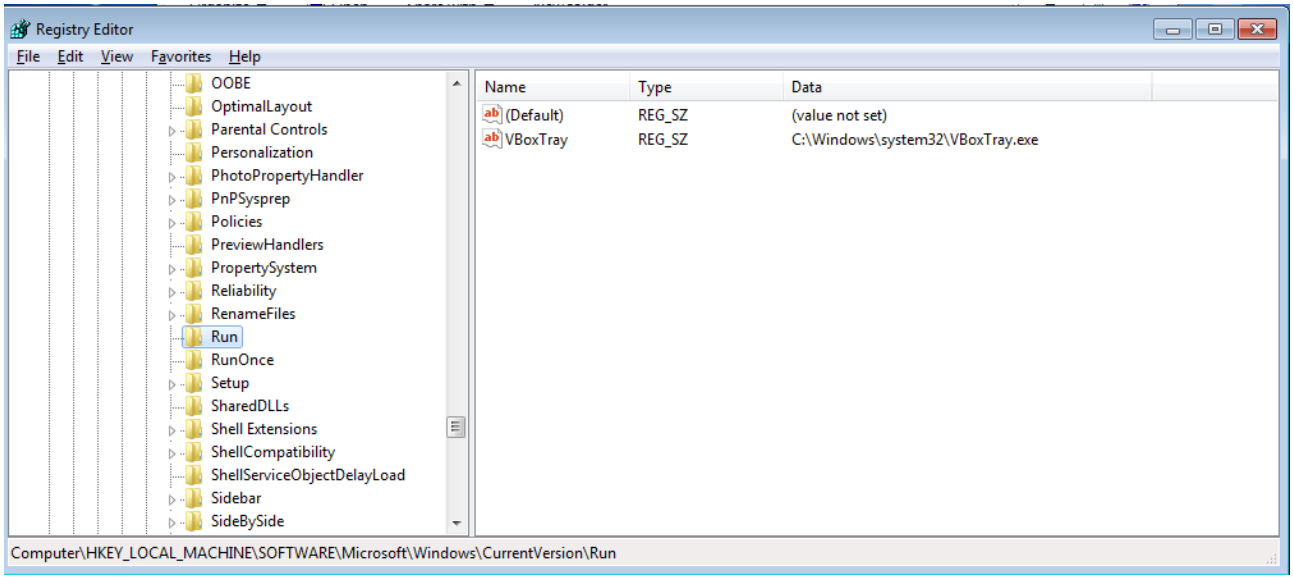
"¿Y esas 5 que aparecen allí? Yo también tengo las mismas."

Bueno esas 5 son las **predefinidas**, o **principales**. Veamos la funcionalidad de cada una:

- **HKEY_CLASSES_ROOT:** Define qué programa abre cada extensión. Si aparece un archivo .doc, esta clave es la encargada de decir "¡Ábrelo con Word!"
- **HKEY_CURRENT_USER:** Configuraciones del sistema operativo del usuario actual que está usando la máquina.
- **HKEY_LOCAL_MACHINE:** Configuraciones de software, hardware y demás de todas las cuentas de usuario.
- **HKEY_USERS:** Datos sobre cada perfil de usuario en el sistema.
- **HKEY_CURRENT_CONFIG:** Información del hardware del equipo.

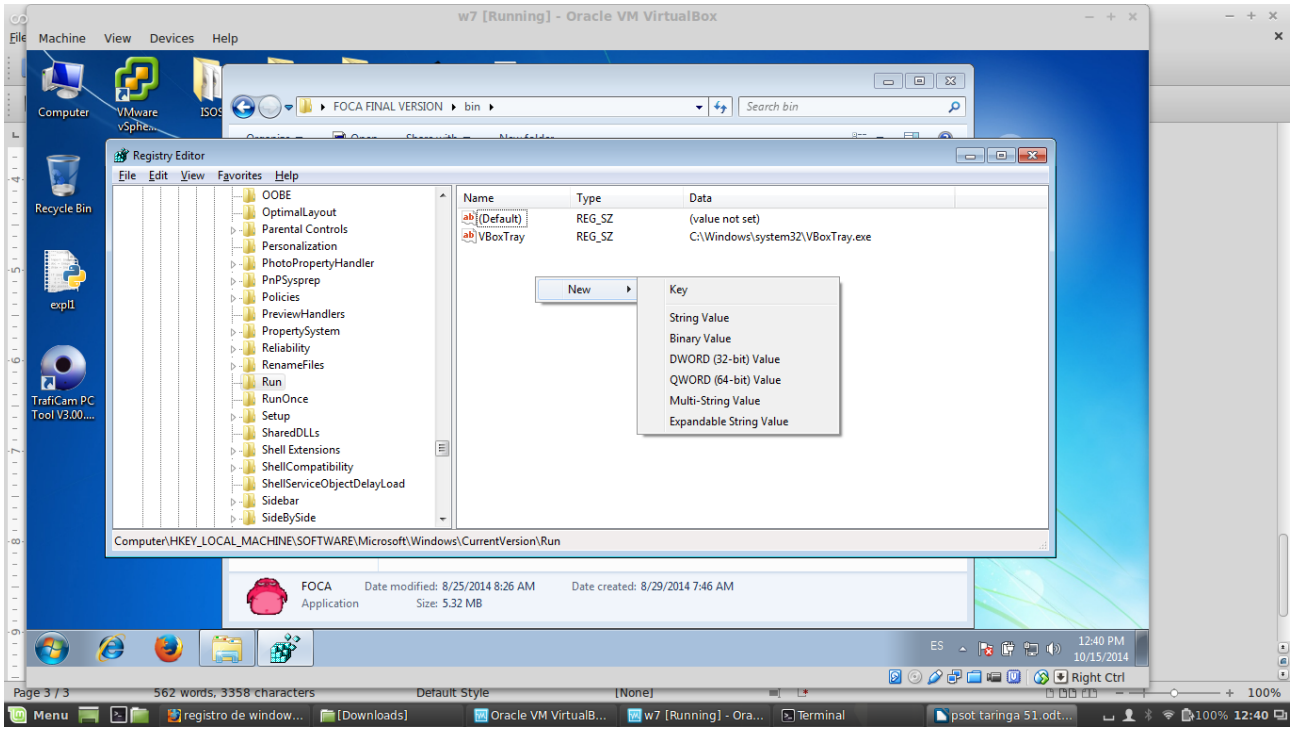
"Allí hay cosas sensibles, de verdad"

Claro. Intentemos de no tocar de más que los errores pueden pagarse en grande aquí. Ahora vamos a ir al directorio donde aparecen los programas al inicio.
La ruta sería: **HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run**. Le damos un click en la clave Run, y nos mostrará los valores que serían los programas que inician con el sistema. En mi caso sólo tengo uno, y corresponde con un valor de la máquina virtual (lo estoy corriendo allí), pero si lo hacen en su máquina host, seguro tengan más.

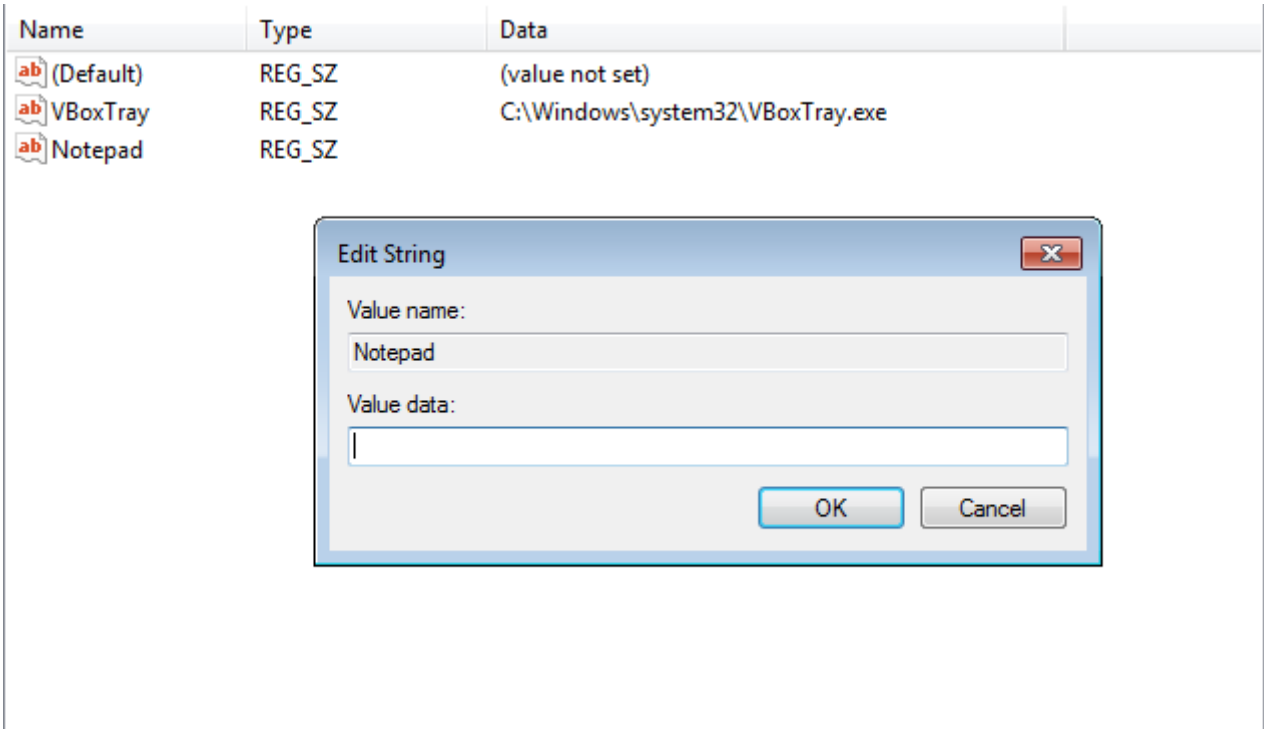


En la imagen, en la columna de "**Data**", a la derecha, aparece la ruta completa del programa que se ejecuta. Si hay algo que no lo queremos allí, le podemos dar click derecho y **eliminar**. Pero en otro caso, para hacer que un programa nuestro se ejecute con el sistema, podemos agregarlo. Veamos como.

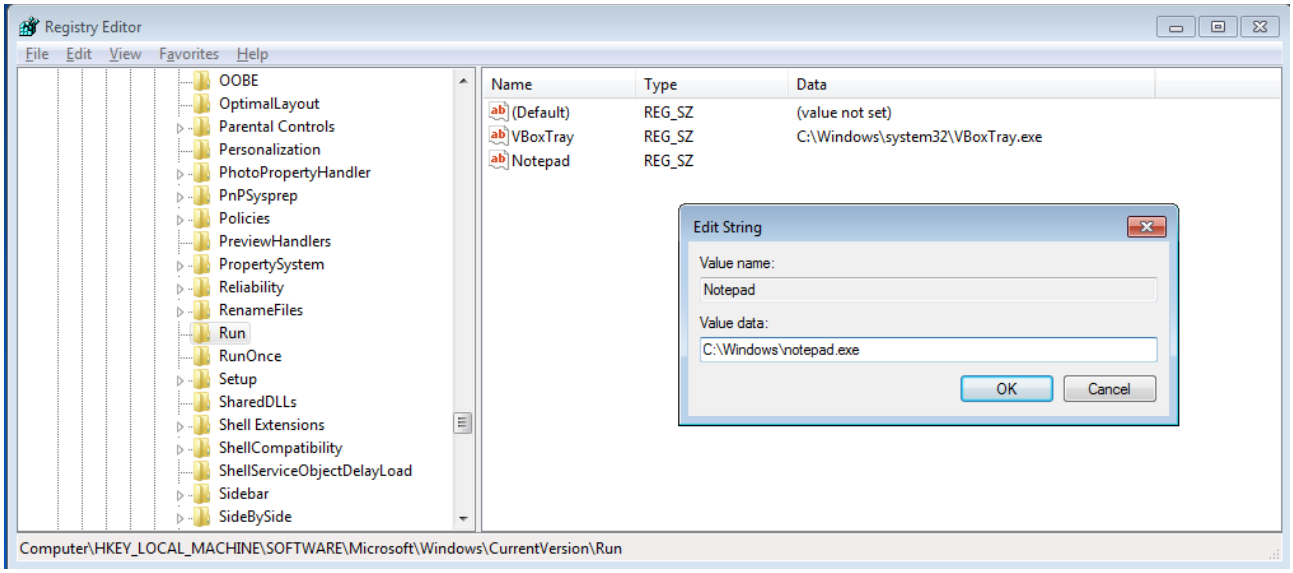
Primero vamos al panel derecho y le damos al click derecho del mouse, elegimos la opción **New String Value.**



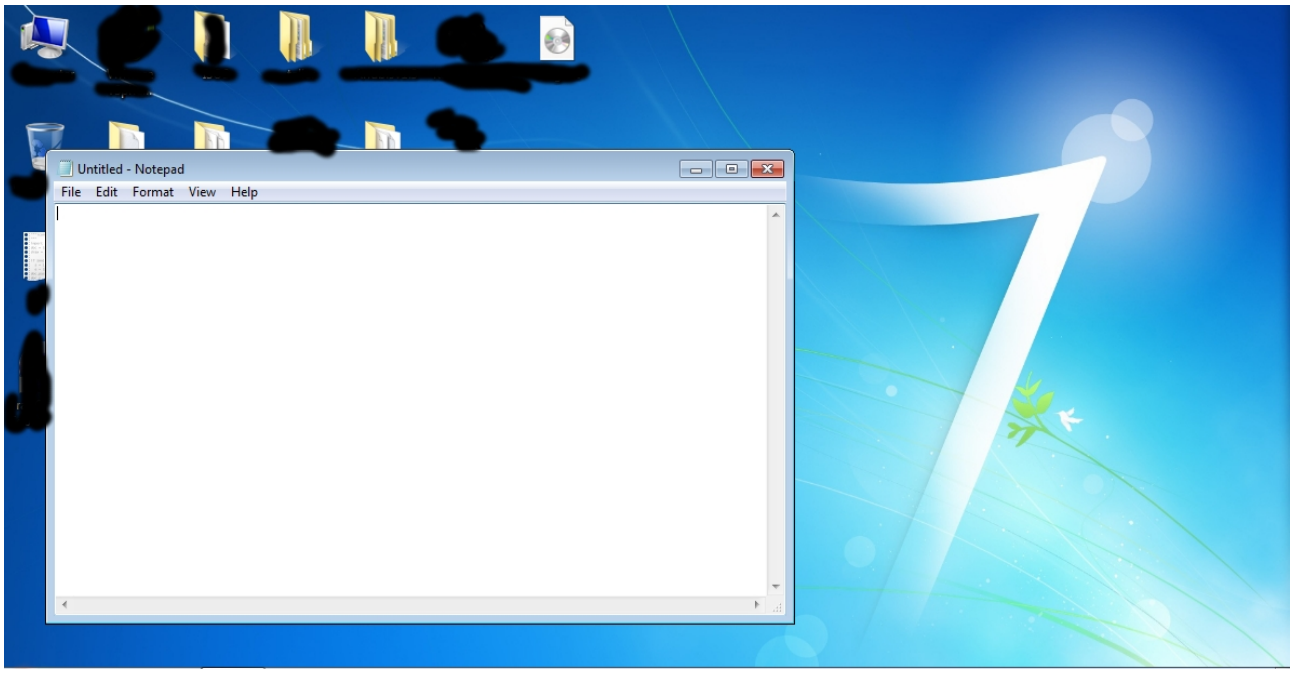
Vamos a darle un nombre cualquiera. En mi caso voy a hacer que se ejecute el Notepad, así que le daré de nombre lo que corresponde, y luego, dándole doble click podemos editarlo.



Claramente, aquí va la ruta del programa a ejecutar.



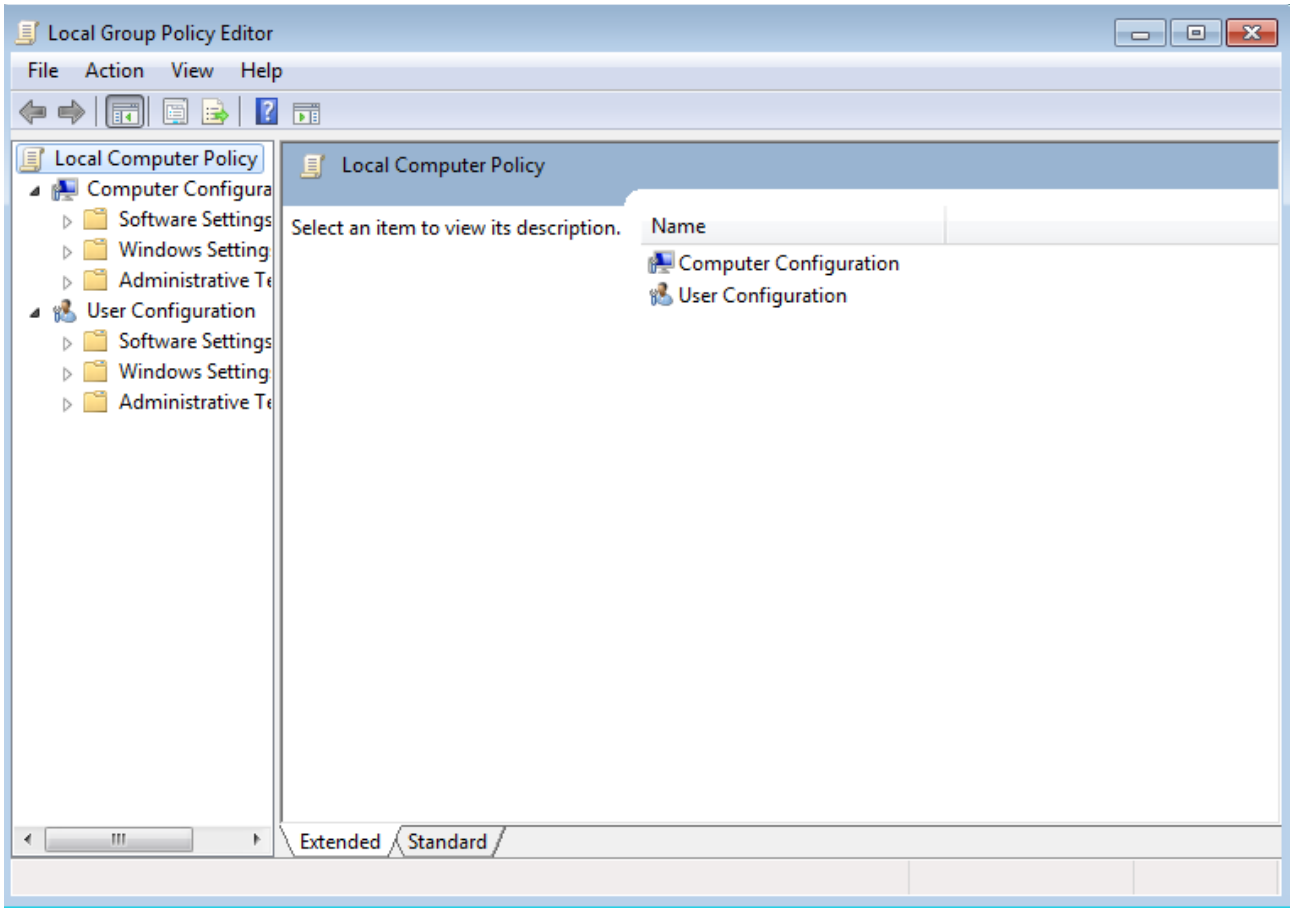
Aceptamos los cambios y cerramos el registro. Reiniciemos el sistema para comprobar el funcionamiento de nuestra edición.



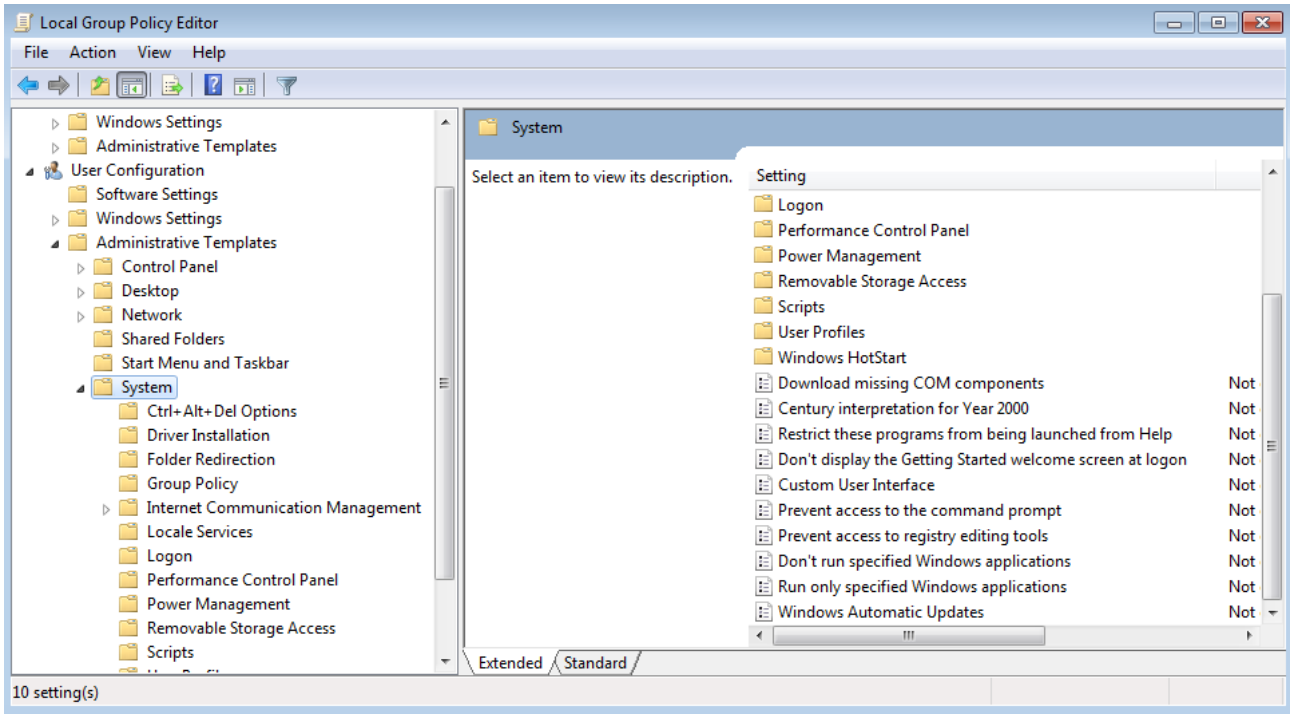
¡Funcionó perfectamente! Así como podemos ver que el notepad inició, podremos hacer que un virus lo haga y ocupe ese lugar en el registro.

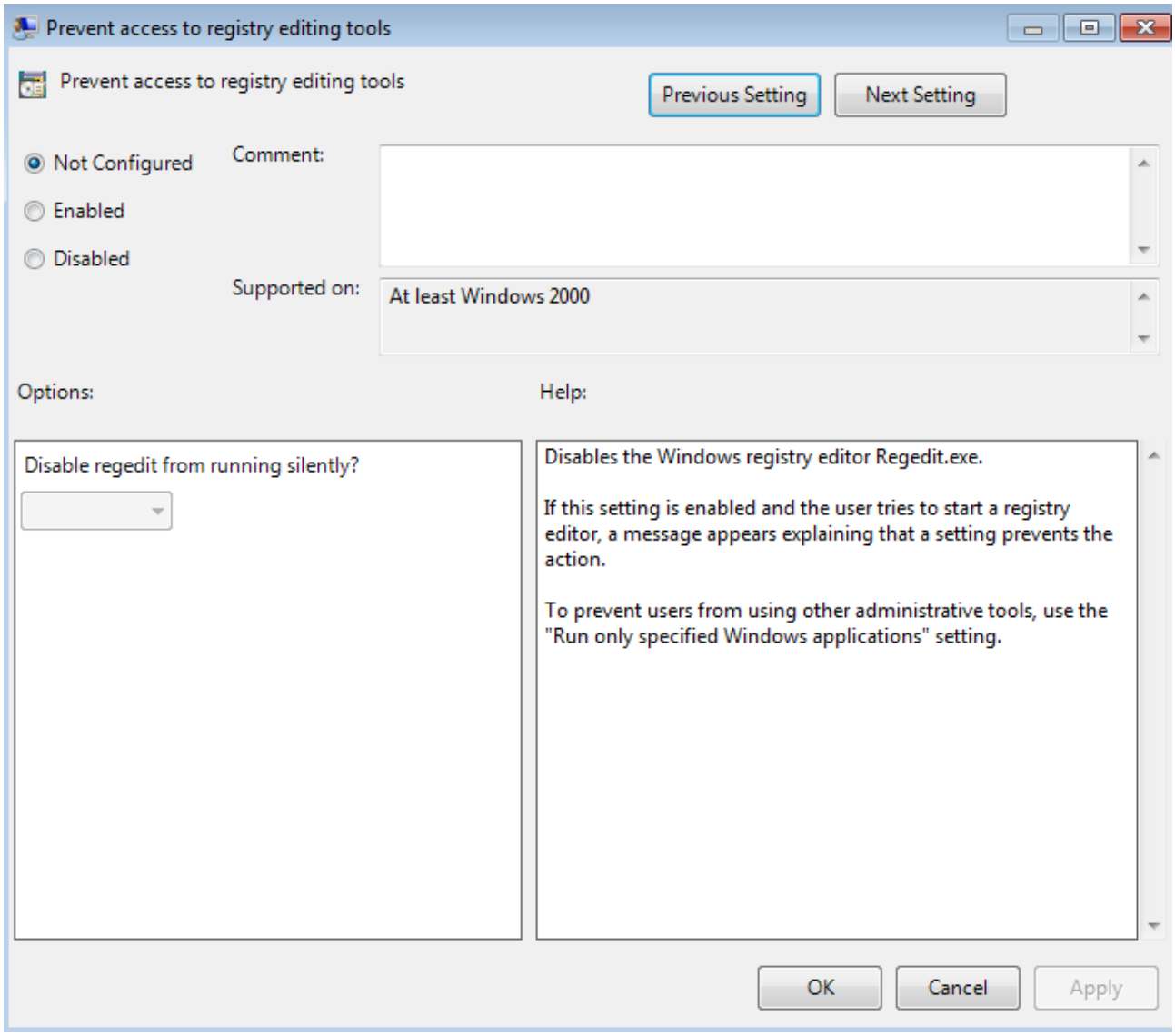
Miremos un truquito más que algun tipo de persona o malware, puedan usar.
Volvamos a **Ejecutar** y escribimos **gpedit.msc.**

Se nos abrirá el editor de las **directivas de grupo** (**local group policy editor**), digamos que aquí se controlal los accesos de cada usuario y qué puede o no puede hacer.

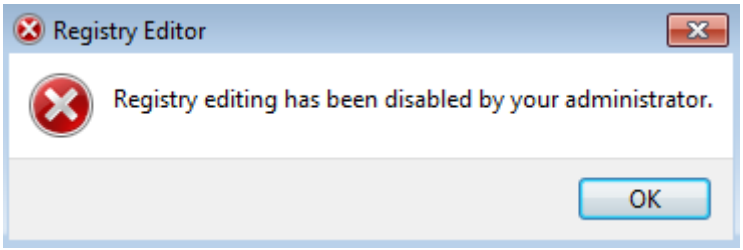


Vamos navegando por el panel de la izquierda. User Configuration -> Administrative Templates -> System. Vamos a ver que en el panel de la derecha, vemos un item llamado "Prevent access to registry editing tools." al que le vamos a dar doble click.





Esto es así, si activamos (enable) vamos a hacer que el usuario no pueda ingresar al regedit. Veamos qué sucede. Démosle al enable y apliquemos los cambios. Luego intentemos de abrir el regedit.



Error. No nos deja. Esto puede ser aprovechado por una persona con malos hábitos para que no puedas cambiar la configuración del registro y hacer que su malware no se ejecute más al inicio del sistema.
Dejémos todo en Disabled y aceptemos para no tener problemas con ésto.

Claro que esto es una de las cosas más burdas que suceden, pero siempre hay que saber las herramientas con las que cuenta el sistema.

Pueden seguirme en Twitter: @RoaddHDC

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente: 1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
