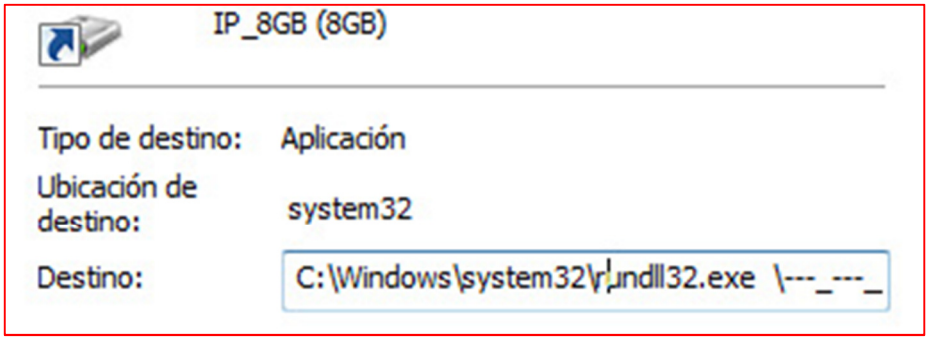
¿Les parece familiar la siguiente imagen?

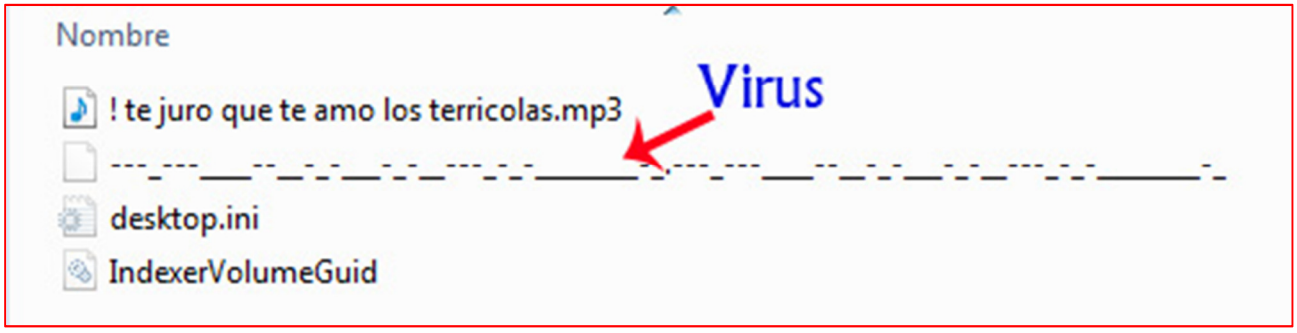
Este virus ya me tenía cansado. Cada vez que me traían una PC para limpiarla, tocaba formatearla. ☺

Observemos las propiedades del acceso directo.



C:\Windows\system32\rundll32.exe \---_---____--__-_-___-_-__---_-_-_____-_.---_---____--__-_-___-_-__---_-_-_____-_,T1Z7jHtR3b9lNvTl

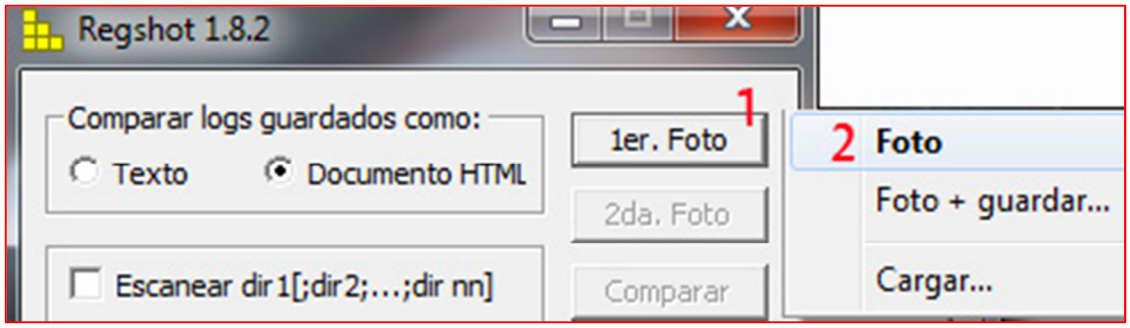
Hay un archivo sin extensión. Cuando el usuario le da clic, ejecuta el virus y abre la carpeta normalmente.



Como tengo la PC congelada con DeepFreeze, la reiniciaré para que quede sin el virus.

Tomaré una foto del registro de Windows antes de ejecutar el virus, usando RegShot v1.8.2

https://sourceforge.net/projects/regshot/files/regshot/1.8.2/regshot_1.8.2_src_bin.zip/download



Ahora ejecuto el virus dándole clic al acceso directo de mi USB.

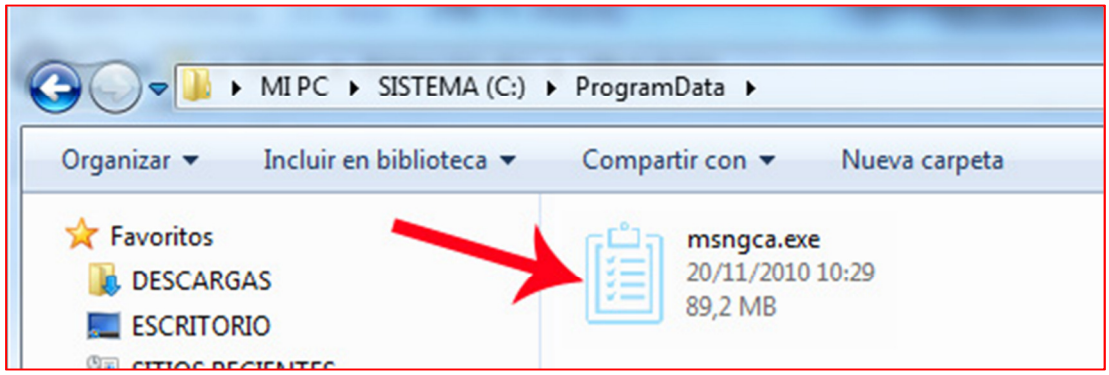
Luego, le tomo la segunda foto y le doy a comparar.

Vemos cosas interesantes como, por ejemplo, la dirección de un ejecutable en el inicio de Windows.

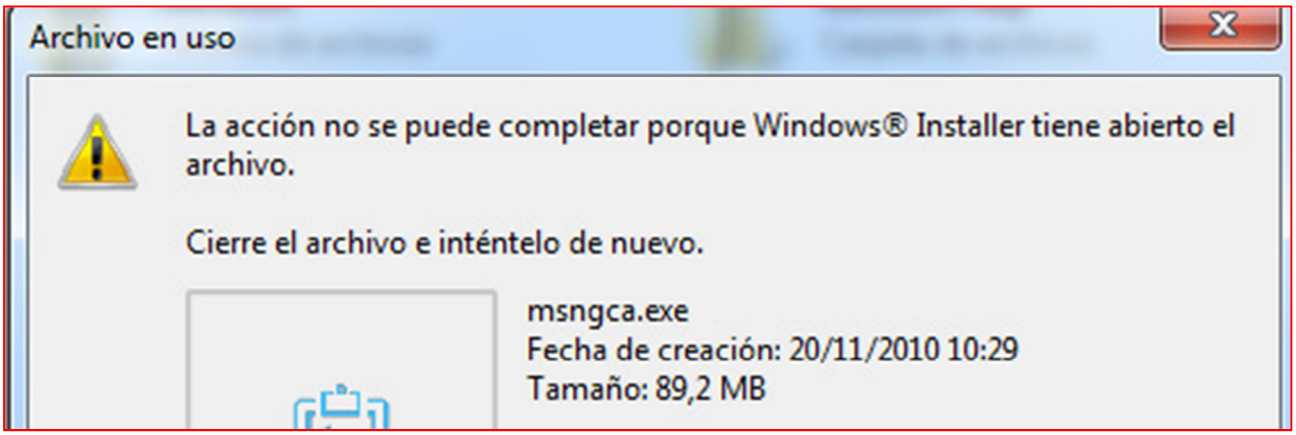
Valores añadidos:47

HKLM\SOFTWARE\Microsoft\WBEM\WDM\USBSTOR\Disk&Ven_hp&Prod_v165w&Rev_1100\AE8CHYE1100003644&0_0-{05
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\1272961301: "C:\ProgramData\msngca.exe"

C:\ProgramData\msngca.exe



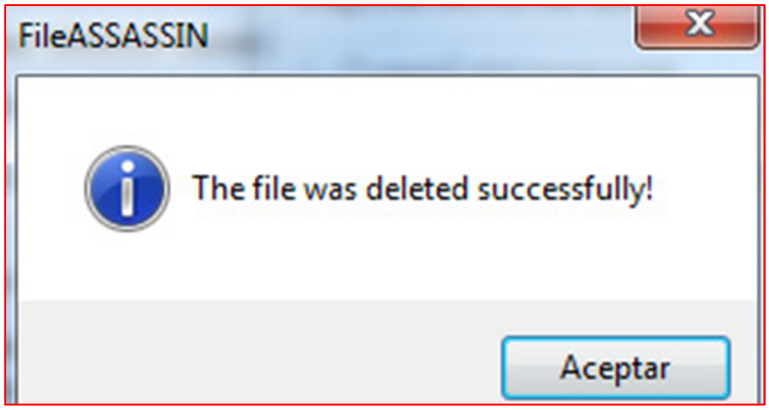
Si vamos a **ProgramData** e intentamos eliminarlo, dice que está siendo usado y ni con **Unlocker** lo podemos eliminar.



Siempre, tenemos que buscar opciones. En este caso, usaremos FileAssasin: http://downloads.malwarebytes.com/file/fileassassin/

Marcamos las opciones como está en la imagen y damos en **Execute**.

Nos dirá que el perro fue eliminado. ☺



Nota: el nombre del virus es variable, pero como en ProgramData no hay exe sino carpeta, es fácil encontrarlo, ya que es el único.

Fin del minitutorial. Espero que ustedes aprovechen este material para ahorrarse un dolor de cabeza.

@IvinsonCLS