*E-mail:* fjweb@hotmail.es

*Mi Web:* http://www.fjweb.es

# Ransomware

## (Encriptador de Archivos)

Hoy vamos a hablar de una de las amenazas más peligrosas para nuestros documentos.

El **Ransomware** es un programa malintesionado que **encripta** nuestros archivos para luego pedir un **rescate para liberarlos**. La encriptación utiliza dos claves, una local y otra que pone el programa, con lo cual es casi imposible recuperar los archivos.

Este tipo de programas se introduce en nuestros ordenadores a través de otros programas descargados de lugares poco seguros. También se introduce al abrir archivos Zip, Rar, etc descargados también de lugares poco seguros.
Otra forma de introducción es a través de correos electrónicos que te indican que has ganado un premio, etc y te piden que entres en enlace Web. Uno de estos correos te comunicaba que tenías un paquete en correos y que no te habían podido entregar y te dan un enlace Web.
Bueno estos sistemas pueden variar y pueden ser enviados por contactos tuyos que estén infectados o Empresas como Endesa, Correos, Etc.
Quiero Recordar que estas Empresas no te los Mandan, son copias ilegales que utilizan sus Nombres para conseguir engañarte.

**Más Información en:**
**Wikipedia**: https://es.wikipedia.org/wiki/Ransomware
**Computer Hoy**: http://computerhoy.com/noticias/software/que-es-ransomware-como-evitarlo-6642
**Softonic**: http://articulos.softonic.com/virus-ransomware-2016-secret-level

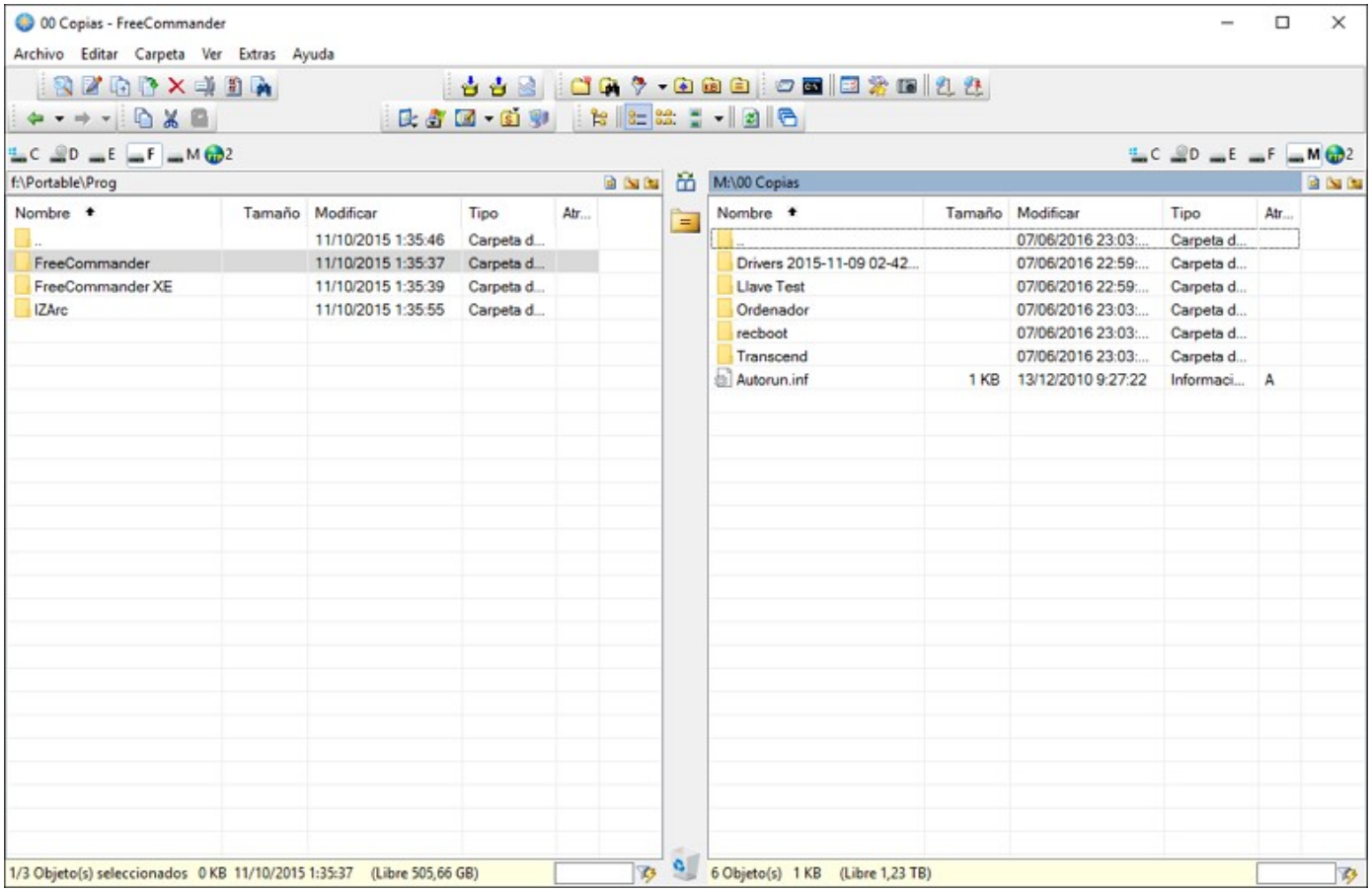
**Algunos Tipos de Ransomware**
CryptoLocker, CryptoLocker.F, TorrentLocker, CryptoWall, TeslaCrypt, Ransom32, Rower3254, Surprise ...
CTB-Locker, ZeroLocker, Variables de DMA Locker, CryptoXXX, CryptoJoker, etc, etc
La cantidad de programas de este tipo es interminable.

**¿Qué se puede hacer?**
**Lo Primero** que debes hacer es tener o comprar un **Disco USB**, en el que guardaremos copias de Seguridad de Windows, Imagen del Sistema. Copias de todos nuestro archivos, Fotos, videos, documentos, datos correo, claves de nuestros programas, etc, etc.
Entramos en el Correo, limpiamos todos los correos no necesarios y creamos una copia de nuestros correos.
En dos palabras todo lo que te interese, por si tuviéramos que reinstalar el Sistema Operativo.

**Antes de Conectar el Disco** y crear estas copias, debemos **pasar el antivirus** a todo el PC, pasar el **Malwarebytes** (actualizado).

Hacer una limpieza de archivos temporales y registro (**Advance Sistem Care y CCleaner**). Una vez el Ordenador limpio apagamos el PC, **desconectamos de Internet** y arrancamos. Conectamos el **Disco USB** y procedemos a crear la **copia del sistema y la Imagen del Sistema** (Solo Archivos del Sistema, Office y Programas Seguros) **en el Disco USB**, después **copiamos Nuestros archivos** en una carpeta en el USB, no te olvides de ninguno importante.

Para copiar archivos es interesante utilizar un programa de dos pantallas ejemplo WinComander (Pago) o FreeCommander (Gratuito)
Es mucho más sencillo al ver lo que copias y donde lo copias.




Una vez tengamos todas las copias hechas, apagamos el PC, desconectamos el USB y arrancamos el Sistema. **El Disco USB lo dejaremos desconectado siempre**. Cuando tengamos que realizar copias nuevas volveremos a realizar la limpieza, conectamos el Disco, copiamos los archivos y volvemos a desconectarlo.

Siempre recuerda desconectar internet antes de conectar el Disco USB. Así si pasa cualquier infección nuestros archivos los tendremos Limpios y Seguros.

**Lo Segundo** que tenemos que hacer es tener un Disco de Recuperación del Sistema **CD/DVD o USB que arranque con un Sistema operativo**.
Ejemplo: Windows XP, Windows 7 o Linux (Si conoces el Sistema)
Después Prepararemos una llave USB con programas para limpiar este tipo de Archivos:
Ejemplo: MalwareBytes, AdwCleaner, ComboFix, Polifix, etc.

También podemos utilizar un Live CD de Antivirus:
**Descarga ISO Antivirus**:
**Karpesky:** http://support.kaspersky.com/viruses/rescuedisk
**Avira:** http://www.avira.com/es/download-start/product/avira-rescue-system
**AVG:** http://www.avg.com/es-es/download.prd-arl
**BitDefender:** http://download.bitdefender.com/rescue_cd/2013/
**Panda:**
http://www.pandasecurity.com/homeusers/downloads/docs/product/help/is/2014/sp/241.htm

**HirensBoot CD** con todo tipo de útiles de Mantenimiento, limpieza y Eliminación de Virus
**HirensBoot CD**: http://www.hirensbootcd.org/download/

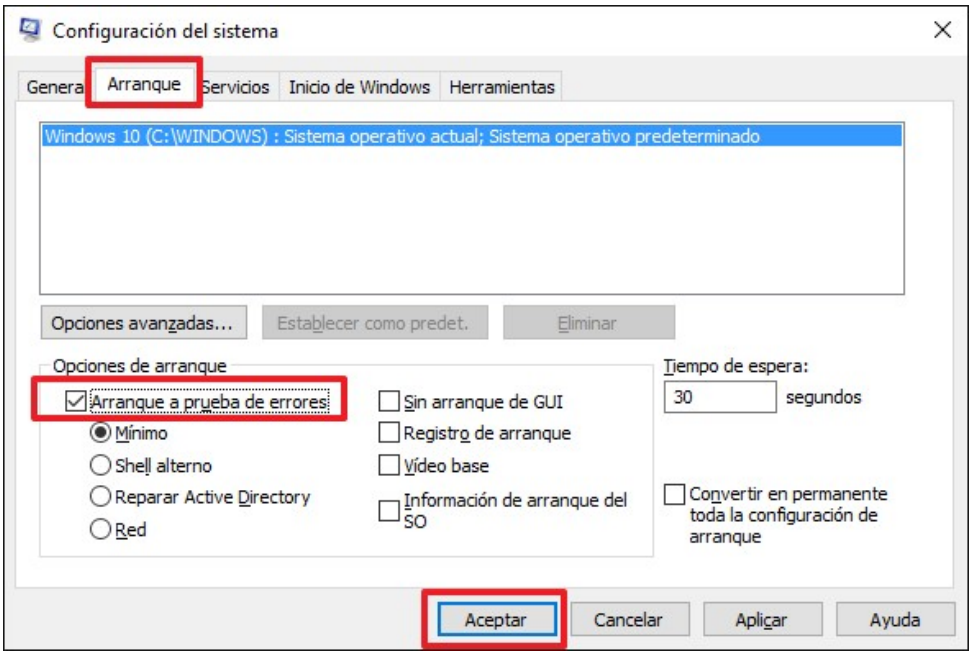
Si tuviéramos que **limpiar el Ordenador** por una infección de este tipo, **metemos el CD/DVD** arrancamos el Ordenador entramos en la **Bios** (F2, Esc, Del ... dependiendo del Ordenador) y en el **Boot** ponemos **arrancar desde el CD/DVD.** Pulsamos **F10 / Guardar y Reiniciar**.
Cuando tengas arrancado el Sistema ejecutas los programas para limpiar el PC.

Una vez Limpio volvemos a la bios y ponemos el Boot como escaba y guardamos, reiniciamos el Sistema. Comprobamos pasando otra vez el Malwarebytes y el AdwCleaner, que no hay infección. Cuando estamos seguros de que no hay infección, borramos y copiamos los archivos encriptados. Listo seguimos funcionando.

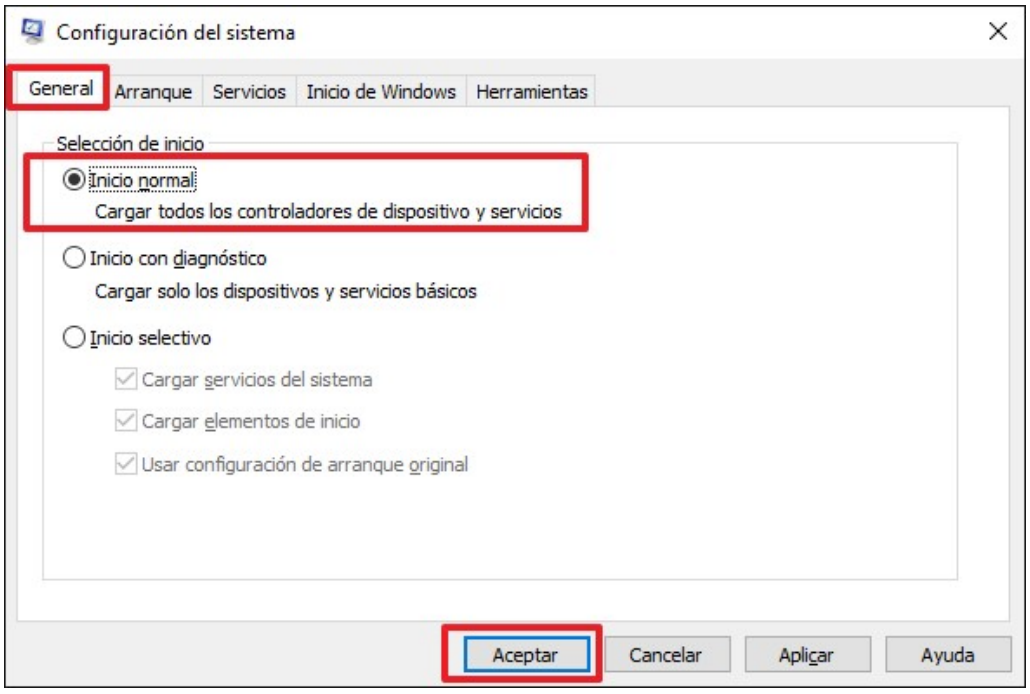
**Nota:** Si no estás seguro es preferible borrar y reinstalar el Sistema Operativo.

**Otra Opción es entrar en Modo Seguro** y ejecutar los programas necesarios, pero algunos de estos bichos impiden la entrada en Modo Seguro. Para entrar en Modo Seguro reiniciamos el PC y pulsamos F8 varias veces hasta que ponga un listado en el que nos de la opción de Modo seguro.

También podemos ir a **Ejecutar y escribimos msconfig**, pulsamos **Intro**.




Vamos a la Pestaña **Arranque** y Marcamos a **Arranque a prueba de Errores**, pulsamos **Aceptar** El ordenador te pedirá Reiniciar. Reinicia.
Realizamos la limpieza y nos aseguremos de que el Bicho esta eliminado.
Cuando terminemos volvemos a **Ejecutar - msconfig** y ponemos los parámetros normales.
**Desactivamos la opción Arranque a prueba de errores**




Vamos a la pestaña **General** y Marcamos **Inicio Normal** y pulsamos en **Aceptar**
Te pedirá reiniciar el Sistema, Reinicia.

Ante todo Recuerda que los archivos Encriptados no los podrás recuperar.
Dicen que hay opciones como ESET, pero no lo sé.
Lo Bueno es que nuestros archivos los tendremos guardados, borramos los archivos encriptados y copiamos los archivos de nuestras copias.

Asegúrate de que esté limpio antes de Conectar el Disco USB.

**Opciones para detectar o protegernos este Tipo de Bichos.**

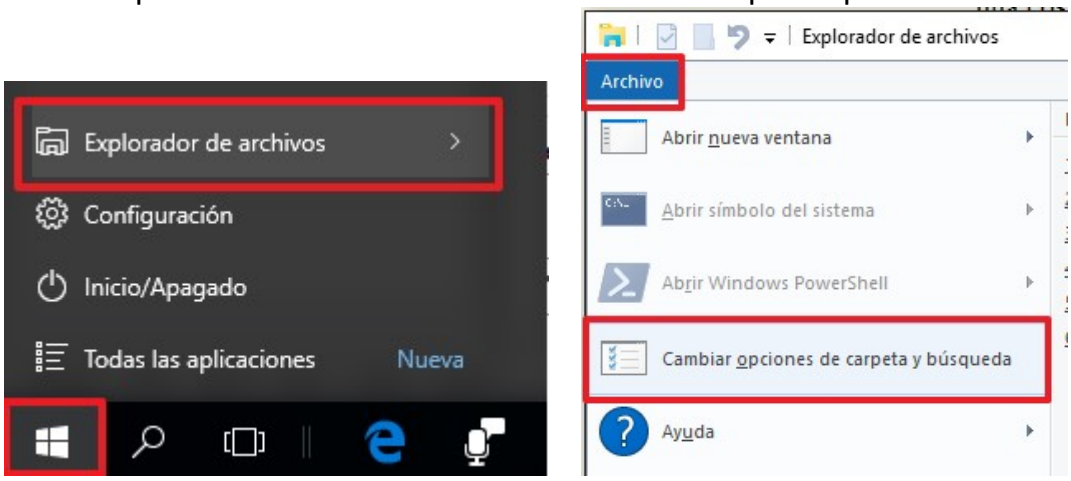
Lo más importante para evitar al máximo una infección de este tipo es asegurarnos que descargamos y de dónde. Algunos programas, zip, rar, imágenes, etc pueden esconder estos bichos, ya que aunque nosotros creamos que es una cosa puede ser otra. Ejem. Fiesta. pdf, en el explorador lo veremos como un archivo pdf pero puede que no sea así y en realidad se llame Fiesta.pdf.exe, al abrirlo ejecutamos el instalador y se abre el archivo pdf, nosotros no nos daremos cuenta de la instalación del bicho porque veremos el pdf pero la instalación se realizara ocultamente y comenzara a ejecutarse al momento.

Si nos damos cuenta de algo así, lo más importante es apagar el PC inmediatamente para evitar que encripte los mínimos archivos posibles y luego como he dicho meter el USB de Arranque para limpiarlo.

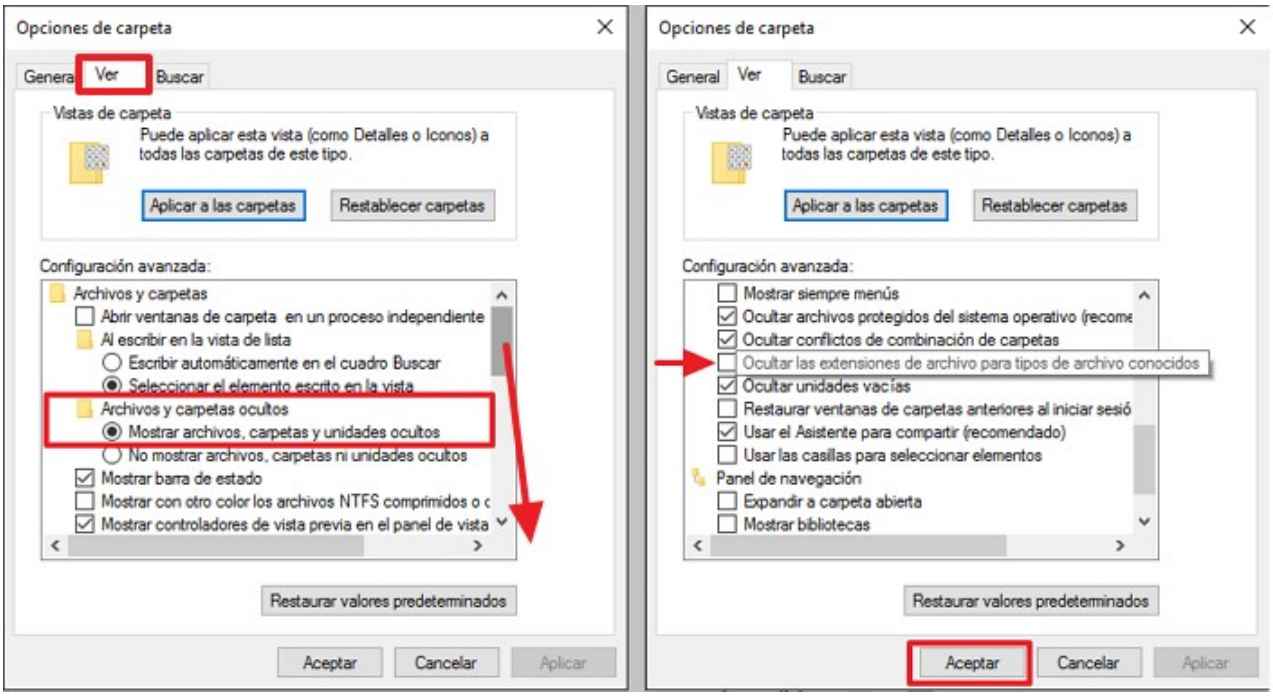
Para poder ver esa segunda extensión realizamos un cambio en el Explorador de Windows.

**Win7:** Botón **Inicio / Panel de Control / Apariencia y Personalización / Opciones de Carpeta.** Pulsamos Clic en la pestaña **Ver** y después en **Configuración Avanzada**: Desmarcamos la Opción: **Ocultar las extensiones de archivo para tipos de archivo conocidos** después pulsamos **Aceptar**. Ahora veremos Fiesta.pdf.exe

**Win10:** Pulsamos en El Botón Inicio / Explorador de Windows /Archivo /
Pulsamos en Cambiar opciones de carpeta y búsqueda / Opciones de carpeta / Ver
Desmarcamos la Opción : Ocultar las extensiones de archivo para tipos de archivo conocidos

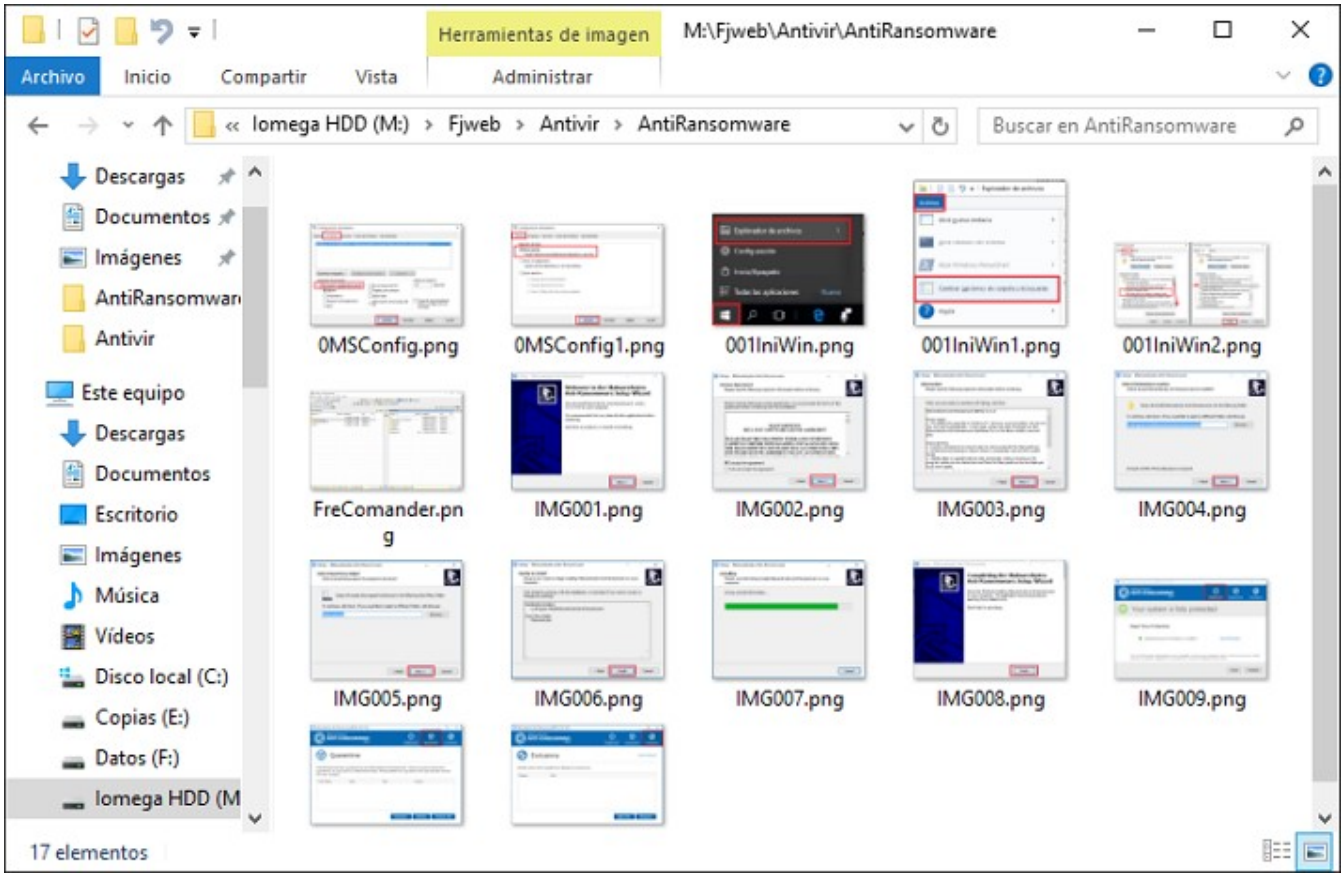



**Inicio / Explorador de Windows /Archivo / Cambiar opciones de carpeta y búsqueda/**




**Opciones de Carpeta / Ver /Desmarca: Ocultar las extensiones de archivo para tipos de archivo conocidos.** Pulsamos en **Aceptar**

**Nota:** La opción **Mostrar archivos, carpetas y unidades ocultos**, yo lo activo para ver los archivos temporales y de las carpetas Ejemplo AppData, Pero cuidado con lo que tocas.




Como puedes ver detrás del archivo aparece la extensión completa.
Ahora cuando descargues algo, antes de ejecutarlo, vas a la carpeta de descarga y compruebas la Extensión.

Esta es una de las prevenciones básicas, otras son no abrir enlaces, si no estás seguro, ni en el correo ni en las Redes Sociales.

Descarga los archivos de las páginas originales, no de páginas dudosas.
Y sobre todo mantén tu Máquina limpia, Pasar Antivirus, Antimalware y limpieza de archivos basura etc.

Nota hay algunos programas Anti Ransomware, pero están en Opción Beta.
En el Siguiente Manual Hablaremos de uno de ellos **Malwarebytes Anti-Ransomware Beta7**

Bueno hay bastantes más opciones y problemas pero creo que lo más importante lo hemos visto.

**Más Información**:
http://blog.elhacker.net/2016/04/como-evitar-prevenir-que-un-ransomware-cifre-secuestre-los-ficheros-archivos-en-servidor-windows.html

Y con esto acabamos el Manual. Espero que os guste el Programa.

Un Saludo, Fjweb.



**Fin del Manual**

Bueno espero que os guste y os funcione bien.
Si tenéis alguna duda,
Mándame un correo a fjweb@hotmail.es

Un Saludo, Fjweb

**Mi Web Informática a nivel Usuario**: http://www.fjweb.es
**Visita en Facebook**: https://www.facebook.com/FjPcFacil/
**Visita mi Blogger**: http://fjweb.blogspot.com.es/