

# BINDERS

**Muchas veces somos engañados con la acción de un binder. Por ello es conveniente conocer estos programas que cualquiera puede utilizar para ocultar un troyano ante otro archivo de apariencia inofensiva. Conozca los binders de primera mano y pruébelos para saber exactamente qué pueden hacer. Dentro de unos días subiremos los primeros a la web.**

---

Estos programas son muy interesantes para infectar inadvertidamente a la víctima con virus y troyanos. Un **binder** (también llamado **Joiner** o **Juntador**) es un programa que une dos o más archivos. Estos archivos pueden ser ejecutables o de cualquier otro tipo dependiendo del **binder** que usemos.

Hay ciertas normas que nunca se pueden violar en este tipo de uniones de archivos. Por ejemplo, podemos unir un archivo **\*.exe** a un archivo **\*.jpg**. Esta unión es factible en **binders** como el **Juntador Beta**, pero el resultado nunca podrá ser un archivo **\*.jpg**.

Si bien un archivo de imagen podría ocultar un ejecutable en su interior, nunca podríamos ejecutar el ejecutable al picar sobre la imagen. Esto hace más difíciles las cosas, pero no hay que desanimarse.

Lo principal es que el **binder** sea capaz de pasar inadvertido ante los antivirus. La pregunta sería si un **binder** es realmente un código maligno. La respuesta es que no: el **binder** no es un troyano, ni un virus, ni estropea nada en el disco duro de un ordenador. Más bien se parece a esos programas inofensivos que circulan por la internet que parte un gran archivo en pequeños trozos para después pegarlos y así recomponer el archivo.

Se pusieron muy de moda estos programas en la época en la que no existían los **CD ROM**. Imagínense Ustedes los problemas que existían cuando había que manejar programas de una extensión superior a la capacidad de un disquete.

Mediante estos programas se podía partir el programa a trasladar en varios trozos que cupieran en varios disquetes y luego fundirlos otra vez en el disco duro. Pues bien, el **binder** sólo utiliza la segunda parte; es decir, la parte de la fusión de archivos. Claro, esto ya puede presuponer aviesas intenciones por parte de las compañías antivirus.

Nos podemos preguntar para qué necesitamos un **binder**. Bueno, es posible adosar mediante uno de estos programas varios archivos **\*.dll** a un ejecutable con la intención de ejecutarlo todo al mismo tiempo, pero no está muy claro esto. Normalmente las compañías antivirus imaginan que debajo de un **binder** hay troyanos, virus o gusanos. De esa manera, tienden a identificar estos programas como *malware*.

Esto dificulta la infección por medio de **binders**, pero hay posibilidades de infectar. Otra posibilidad son los llamados **droppers**, que resultan mucho más difíciles de detectar, pero necesitan programas como **DCC-32** para recompilar el virus. Aún así son también detectados y su tiempo de "vigencia" es limitado.

Aquí mi recomendación personal me lleva a aconsejaros que no usen Ustedes **binders**, a menos que sea absolutamente necesario. Y es que el antivirus más tarde o más temprano acabará detectándolos y pueden tener Ustedes problemas con la persona a la que han infectado si al final identifican el archivo infectado con su autor.

Antes de usar uno de estos programas lo mejor es probarlo en el propio ordenador con archivos inofensivos. Algunos **binders** permiten engañar a la víctima cambiando el icono del servidor por un icono propio de una imagen **\*.jpg**, una carpeta o un documento de texto.

El problema es que luego la extensión, como apunté antes, no puede cambiarse también. Está el pequeño truco de utilizar la doble extensión: en algunos ordenadores funciona este truco porque ocultan por defecto la extensión **\*.exe**.

En un caso así la víctima tiene todas las posibilidades de ser engañada. Es cuestión de suerte.

A continuación voy a describir los más importantes ( pulsa en el título para descargar ):

## **ZenythBinder**

Binder de la casa hecho por HypNosS, su funcionamiento es simple seleccionar dos archivos y dar a juntar. Se creará el ejecutable **zenyth.exe** en la misma carpeta. Ese es el archivo resultante. Se pueden juntar 2

txt's el resultado es un exe que al ejecutarlo abre los 2 txt's con la aplicación que tengan asignada por defecto, en mi caso el notepad.exe

### **Hammer Binder v3.0**

Uno de los binders mas completos, tiene muchas opciones, desde juntar archivos, a añadir claves de registro, ejecutar parametros. Esta version es muy al estilo de delphi u otra interfaz grafica de programación. Quizas os resulte difícil usarlo, así que os voy a dar los pasos básicos para manejarlo.

Primero damos sobre el icono de bind file (el del clip), ahora en el object inspector, a la izquierda damos sobre source file y seleccionamos el archivos que deseamos juntar. Ahora editamos el resto de propiedades: *ExecMethod*: *None* no se ejecuta, *AsyncHidden* asíncrono y oculto, *ShellHidden* consola oculto. Yo he probado con *AsyncHidden* y todo a ido bien.

*ExecParams*: Parametros con los que se ejecuta el archivo, útil con serv-u que hay que pasarle por parámetros el fichero de configuración por ejemplo...

*Attributes, name, options*: no hay mucho que describir

*Registry Startup*: Si queremos que se ejecute el archivo cada vez que se reinicie el ordenador, las mas clásicas son *Run*, *Services*.

*RegistryValueName*: Nombre de la clave en el registro, svchost es un buen nombre, ¿no os parece?.

*RemoteFilename*: nombre con el que se extraera.

*RemoteFolder*: Carpeta donde se extraera.

Ahora pulsad built stub y te dira donde se ha creado el stub.

Como véis hay muchisimas más opciones, eliminar archivo, mostrar mensaje, añadir, borrar, modificar clave de registro. Todo esto lo dejo a vuestra curiosidad.

Aquí tenéis unos cuantos binder mas, sabiendo manejar un par de ellos el resto es igual:

<http://www.trojanfrance.com/index.php?dir=Binders/>

**Autor: Coolvibes**

**Página: [Indetectables.com.ar](http://Indetectables.com.ar)**